# Avaya P550R®, P580, P880, and P882 Multiservice Switch User Guide Version 5.3.1

July 2002

**Avaya P550R®, P580, P880, and P882 Multiservice Switch User Guide, Version 5.3.1**

**© Copyright Avaya Inc., 2002 ALL RIGHTS RESERVED**

**Produced in USA, July, 2002**

The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this document. Avaya disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

P550R is a registered trademark of Avaya Inc.

Microsoft, Windows, Windows NT, Windows 95, Windows 98, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

Sybase is a registered trademark of Sybase, Inc.

Novell, NDS, Netware, and Novell Directory Services are registered trademarks of Novell, Inc.

Solaris is a trademark of Sun Microsystems, Inc.

Intel and Pentium are registered trademarks of Intel Corporation.

ALL OTHER TRADEMARKS MENTIONED IN THIS DOCUMENT ARE PROPERTY OF THEIR RESPECTIVE OWNERS.

# Table of Contents


***Preface . . . . . xiii***

Overview of the Contents. . . . . xiii
Technical Support . . . . . xv
Avaya Technologies Products and Services . . . . . xv
Conventions . . . . . xvi
Using Notes, Cautions, and Warnings . . . . . xviii
Related Documentation . . . . . xviii
Online Documentation . . . . . xviii
Online Help . . . . . xix
Installing Online Documentation and Help Files . . . . . xix
Documentation . . . . . xxii
Terminology . . . . . xxii
Documentation Feedback. . . . . xxiii

***Chapter 1 — Introduction . . . . . 1-1***

Overview . . . . . 1-1
Switch Descriptions . . . . . 1-1
Hardware Components . . . . . 1-2
Chassis . . . . . 1-2
Avaya P550R and P580 Multiservice Switch Chassis . . . . . 1-3
Avaya P880 and P882 Multiservice Switch Chassis . . . . . 1-5
50-Series Modules . . . . . 1-7
Redundant Supervisor . . . . . 1-9
Media Modules . . . . . 1-10
80-Series Modules . . . . . 1-13
Software Features . . . . . 1-14
Virtual Bridging Functions . . . . . 1-14
Flood Pruning Using VLANs . . . . . 1-15
Hunt Groups . . . . . 1-16
OpenTrunk Technology . . . . . 1-16
Load MIB . . . . . 1-17
Spanning Tree Modes . . . . . 1-17
Extensive Fault Tolerance. . . . . 1-21
Buffer and Queue Management. . . . . 1-21
New Software Features . . . . . 1-22
v5.3 Software Features . . . . . 1-22
v5.2.10 Software Features . . . . . 1-25
v5.2.6 Software Features . . . . . 1-26

v5.2.2 Software Features . . . . . 1-27
v5.2.0 Software Features . . . . . 1-27
Routing Overview . . . . . 1-28
Compatibility with Layer 2 Modules . . . . . 1-29
Routing with Layer 2 and Layer 3 Modules . . . . . 1-29

***Chapter 2 — Initialize and Setup . . . . . 2-1***

Overview . . . . . 2-1
Setting Up Your Laptop or PC Monitor . . . . . 2-2
Managing the Avaya Multiservice Switch using Telnet . . . . 2-2
Viewing Active Telnet Sessions . . . . . 2-3
Telnet session expiration timer . . . . . 2-4
Configuring the Supervisor Module Using the CLI . . . . . 2-4
Configuring the Switch Using the Web Agent . . . . . 2-9
Opening the Web Agent . . . . . 2-9
Moving through the Web Agent . . . . . 2-11
Configuring Custom Access Types . . . . . 2-12
Opening the Custom Access Types Web Page . . . . . 2-13
Creating a Custom Access Type . . . . . 2-14
Modifying a Custom Access Type . . . . . 2-15
Deleting a Custom Access Type . . . . . 2-16
Setting Up User Accounts . . . . . 2-17
Disabling User Accounts . . . . . 2-19
Setting Up SNMP Communities . . . . . 2-20
Configuring User Accounts . . . . . 2-23
Remote Authentication Dial-In User Service (RADIUS) Client Support2-24
Changing the Console Serial Port Settings . . . . . 2-32
Configuring the Serial Console Port as a TTY Console . . . . 2-32
Configuring the Serial Console Port as a PPP Console . . . . 2-35
Configuring Dial-Up Networking . . . . . 2-40
Changing the TCP Ports for HTTP and Telnet . . . . . 2-43
Overview . . . . . 2-43
Changing the TCP Port Number for HTTP and Telnet Requests2-43
Starting a Telnet Session . . . . . 2-45
Opening the Web Agent . . . . . 2-46
Managing Configuration Files . . . . . 2-46
Viewing Your Running Configuration . . . . . 2-46
Viewing Your Startup Configuration . . . . . 2-47
Viewing Your Script Execution Log File . . . . . 2-47
Copying Configuration Files . . . . . 2-47
Copying Files . . . . . 2-49
Viewing the Status of a TFTP Transfer . . . . . 2-53

***Chapter 3 — Configuring System Information . . . . . 3-1***

Overview . . . . . 3-1
Entering General System Information . . . . . 3-1
Enabling the Simple Network Time Protocol . . . . . 3-2

Setting Summer Time Hours . . . . . 3-4
Setting Recurring Summer Time Hours . . . . . 3-5
Setting One-Time Summer Time Hours . . . . . 3-9
Setting the System Clock . . . . . 3-10
Setting the Temperature System . . . . . 3-12
Displaying the Power System Statistics . . . . . 3-13
Displaying Cooling System Statistics . . . . . 3-15
Performing a Reset . . . . . 3-16

***Chapter 4 — Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping . . . . . 4-1***

Overview . . . . . 4-1
VLAN Introduction . . . . . 4-1
What is a VLAN? . . . . . 4-2
Ingress Rules . . . . . 4-4
Forwarding Rules . . . . . 4-5
Egress Rules . . . . . 4-7
Creating and Implementing VLANs . . . . . 4-7
VLAN Considerations . . . . . 4-7
Creating a VLAN . . . . . 4-8
Configuring VLAN Parameters . . . . . 4-11
Assigning Ports to VLANs . . . . . 4-13
Spanning Tree Protocol Setup and Monitoring . . . . . 4-13
Spanning Tree Protocol Implementation . . . . . 4-13
Managing the Spanning Tree Protocol . . . . . 4-15
Configuring Spanning Tree Protocol Ports . . . . . 4-20
Disabling Spanning Tree Mode for the Port . . . . . 4-24
Using Hunt Groups to Aggregate Bandwidth between Switches 4-28
Hunt Group Terminology . . . . . 4-29
How Hunt Groups Load Share . . . . . 4-30
Hunt Group Configuration Considerations . . . . . 4-35
Creating Hunt Groups . . . . . 4-36
Adding Ports to the Hunt Group . . . . . 4-37
Viewing Hunt Group Members . . . . . 4-42
Removing Ports from Hunt Groups . . . . . 4-43
Configuring VLAN Trunk Protocol (VTP) Snooping . . . . . 4-44

***Chapter 5 — Configuring Port Parameters . . . . . 5-1***

Overview . . . . . 5-1
Two Categories of Port Parameters . . . . . 5-1
Physical Port Features . . . . . 5-2
Switch Port Features . . . . . 5-5
Relationship Between Different Switch Port Parameters . . . . 5-6
Assigning VLANs to a Port and Associated Issues . . . . . 5-10
Configuring Physical Port Parameters . . . . . 5-12
Configuring Physical Port Parameters on Gigabit Ports . . . . 5-12
Configuring Physical Port Parameters on Fast Ethernet Ports 5-17

Using the All Ports Configuration Window . . . . . 5-23
Configuring Switch Port Parameters . . . . . 5-24
Configuring Switch Port Parameters . . . . . 5-24
Automatic VLAN Creation. . . . . 5-30
Configuring Fast Start Mode . . . . . 5-33
Enabling the Auto Flush Feature . . . . . 5-34
Using the All Module Ports Configuration Window . . . . . 5-36
Viewing Switch Port Parameters . . . . . 5-37
GBIC Identification. . . . . 5-38
Network Error Detection and Recovery . . . . . 5-39
Overview . . . . . 5-39
Enabling NEDR . . . . . 5-42
Internal Error Detection and Recovery . . . . . 5-44
Overview . . . . . 5-44
Enabling IEDR . . . . . 5-45
Enabling IEDR for Hunt Groups . . . . . 5-45
Setting the IEDR Threshold for Internal Errors. . . . . 5-46
Viewing IEDR Settings. . . . . 5-46
Viewing IEDR Settings for Hunt Groups . . . . . 5-46
Error Messages. . . . . 5-47
System Messages . . . . . 5-47

***Chapter 6 — Managing the Address Forwarding Table. . . . . 6-1***

Overview . . . . . 6-1
Relationship between VLANs, AFT and Hash Table Sizes . . . . . 6-2
Hash Table guidelines for creating VLANs . . . . . 6-3
Examples of Configuring VLANs and Hash Table Size . . . . . 6-5
AFT Default Settings. . . . . 6-7
Address Forwarding Table, Auto-Sizing, Auto Increment and Threshold6-7
Total Entries, Address Memory, Age and Super-Age Timers . . . . 6-9
Overview . . . . . 6-9
Configuring the AGE and Super Age Timers. . . . . 6-9
Instance Table Information . . . . . 6-10
Searching the Switch AFT . . . . . 6-15
Adding Entries to the AFT Manually . . . . . 6-21
Option 82 for DHCP . . . . . 6-23
Changing the Status of Option 82 by Using the Web Agent 6-23
Changing the Status of Option 82 by Using the CLI . . . . . 6-23
Changing the Status of Option 82 by Using SNMP . . . . . 6-24
MAC Address Lock and Traps for Unknown Source Addresses. 6-24

***Chapter 7 — Configuring Redundancy Options . . . . . 7-1***

Overview . . . . . 7-1
Configuring Redundant Hardware . . . . . 7-3
Redundant Switch Controllers and Elements . . . . . 7-3
Installing and Enabling Redundant Hardware . . . . . 7-5
Installing Redundant Hardware . . . . . 7-6

Enabling Redundant Hardware . . . . . 7-6
Replacing the Primary Controller . . . . . 7-9
Replacing an Element . . . . . 7-10
Configuring Supervisor Module Redundant Ethernet Console IP Addresses 7-11
Synchronizing the Active and Standby CPUs . . . . . 7-14
Synchronizing Process . . . . . 7-14

## Chapter 8 — Configuring DNS Client . . . . . 8-1

Overview . . . . . 8-1
DNS Client Support . . . . . 8-1
. . . . . 8-9

## Chapter 9 — Configuring IP Routing . . . . . 9-1

Overview . . . . . 9-1
Routing Function . . . . . 9-1
Hardware Requirements for IP Routing . . . . . 9-2
Software Requirements for IP routing . . . . . 9-2
Minimum IP Routing Configuration Requirements . . . . . 9-3
Routing Configuration Quickstart . . . . . 9-3
Displaying Existing IP Interfaces . . . . . 9-4
Creating and Assigning IP Interfaces to the VLAN . . . . . 9-6
Enabling IP Forwarding (Routing) Global Parameters . . . . . 9-11
Access Lists (also called Access Control Lists or ACLs) . . . . 9-16
Access Control List Overview . . . . . 9-17
Creating Access Lists . . . . . 9-21
Activating Access Lists . . . . . 9-28
Example: Filtering Web Traffic Using an Access Rule . . . . . 9-29
Optimizing Performance when Using an Access Control List 9-31
How to Optimize Performance when using ACLs . . . . . 9-33
Evaluate System Performance . . . . . 9-35
Enable Routing at the Module . . . . . 9-37
Design Safe, Efficient ACLs . . . . . 9-37
Identify the Ports . . . . . 9-39
Configuring Hash Mode . . . . . 9-41
Managing F-chip Memory . . . . . 9-41
Creating IP Static Routes . . . . . 9-43
Creating IP Static ARP Entries . . . . . 9-45
Creating a BOOTP/DHCP Server Entry . . . . . 9-46
Option 82 for DHCP . . . . . 9-48
IP Multicast . . . . . 9-50
Configuring IGMP . . . . . 9-51
Configuring and Modifying Distance Vector Multicast Routing Protocol (DVMRP) . . . . . 9-57
Modifying a DVMRP Interface . . . . . 9-59
Monitoring Switch Performance Using IP Statistics . . . . . 9-61
Displaying Global IP Routing Statistics . . . . . 9-62
IP Multicast Statistics . . . . . 9-72

Displaying IGMP Interface Statistics . . . . . 9-74
Displaying the IGMP Group Membership Table . . . . . 9-77
Displaying the IGMP Local Multicast Forwarding Cache . . 9-78
Displaying DVMRP Global Statistics . . . . . 9-79
Displaying DVMRP Interface Statistics . . . . . 9-81
Displaying DVMRP Neighbor Router(s) . . . . . 9-83
Displaying DVMRP Routing Table Statistics . . . . . 9-84
Displaying the DVMRP Route Table . . . . . 9-85
Displaying the DVMRP Upstream Routers . . . . . 9-87
Displaying the DVMRP Designated Forwarder(s) Table . . . 9-87
Displaying the DVMRP Downstream Dependent Router(s) 9-88
Displaying the DVMRP Multicast Forwarding Cache . . . . . 9-89
Configuring Virtual Router Redundancy Protocol (VRRP) . . . . 9-93
Globally Enabling VRRP . . . . . 9-93
Enabling VRRP on an Interface . . . . . 9-94
Creating a VRRP Virtual Router . . . . . 9-96
Displaying VRRP Statistics . . . . . 9-100
VRRP Configuration Considerations . . . . . 9-103
Configuring ICMP Router Discovery Protocol (IRDP) . . . . . 9-106
Enabling IRDP on an Interface . . . . . 9-106
Configuring Lightweight Directory Access Protocol (LDAP) . . 9-109
Configuring LDAP Settings . . . . . 9-109
Viewing LDAP Statistics. . . . . 9-113
Configuring a Static Route for the PPP Console . . . . . 9-115
Configuring the IP Interface for the PPP Console . . . . . 9-116

***Chapter 10 — Configuring the Routing Information Protocol (RIP)10-1***

Overview . . . . . 10-1
Configuring RIP on the Switch . . . . . 10-1
Modifying RIP Interfaces . . . . . 10-4
Creating Trusted RIP Neighbors . . . . . 10-7
Viewing RIP Statistics . . . . . 10-12
NBMA IP Interfaces . . . . . 10-14
Overview . . . . . 10-14

***Chapter 11 — Configuring the OSPF Routing Protocol . . . . . 11-1***

Overview . . . . . 11-1
What is OSPF? . . . . . 11-1
Configuring Open Shortest Path First (OSPF) . . . . . 11-2
Configuring the OSPF Global Configuration . . . . . 11-3
Creating OSPF Areas . . . . . 11-5
Deleting OSPF Areas . . . . . 11-7
Modifying OSPF Areas. . . . . 11-8
Enabling OSPF on an IP Interface . . . . . 11-9
Modifying OSPF Interfaces . . . . . 11-9
OSPF Passive-Interface . . . . . 11-13
Creating OSPF Virtual Links . . . . . 11-14
Deleting OSPF Virtual Links . . . . . 11-16

Modifying OSPF Virtual Links . . . . . 11-17
Creating OSPF Summaries . . . . . 11-18
Deleting OSPF Summaries . . . . . 11-20
Modifying OSPF Summaries . . . . . 11-20
Monitoring Switch Performance Using OSPF Statistics . . . . . 11-21
Displaying OSPF Statistics . . . . . 11-21
Displaying OSPF Links . . . . . 11-24
Displaying OSPF Neighbors . . . . . 11-25
Searching the OSPF Link State Database . . . . . 11-27
NBMA IP Interfaces. . . . . 11-33
Overview . . . . . 11-33
Setting Up an NBMA IP Interface . . . . . 11-34
Setting Up NBMA Neighbors . . . . . 11-35
Removing NBMA Neighbors . . . . . 11-36

***Chapter 12 — Configuring IPX Routing . . . . . 12-1***

Overview . . . . . 12-1
IPX Overview . . . . . 12-1
IPX Datagram Structure . . . . . 12-2
Configuring the Avaya Switch as an IPX Router . . . . . 12-3
Hardware Requirements . . . . . 12-3
Configuring IPX Routing Globally . . . . . 12-4
Configuring IPX Interfaces . . . . . 12-5
Creating IPX Static Routes . . . . . 12-9
Deleting IPX Static Routes . . . . . 12-12
Modifying IPX Static Routes. . . . . 12-13
Creating IPX Static Services . . . . . 12-13
Deleting IPX Static Service . . . . . 12-16
Modifying IPX Static Service . . . . . 12-17
Monitoring Your Switch Using IPX. . . . . 12-17
Displaying IPX Global Statistics . . . . . 12-18
Searching the IPX Route Table. . . . . 12-20
Displaying the IPX Route Table . . . . . 12-21
Displaying IPX Route Table Statistics . . . . . 12-22
Searching the IPX Service Table. . . . . 12-23
Displaying the IPX Service Table . . . . . 12-24
Displaying IPX Service Table Statistics . . . . . 12-25

***Chapter 13 — Configuring IPX RIP Protocol . . . . . 13-1***

Overview . . . . . 13-1
Configuring Internetwork Packet Exchange (IPX) Routing Interface Protocol (RIP) Interfaces . . . . . 13-1
Creating and Modifying IPX RIP Filters . . . . . 13-3
View RIP Interface Statistics. . . . . 13-8

***Chapter 14 — Configuring IPX SAP Protocol. . . . . 14-1***

Overview . . . . . 14-1

Configuring Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP) Interfaces . . . . . 14-1
Creating IPX SAP Filters . . . . . 14-3
Creating IPX SAP Name Filters . . . . . 14-4
Creating IPX SAP Network Filters . . . . . 14-8
Interpreting IPX SAP Interface Statistics . . . . . 14-13

***Chapter 15 — Configuring AppleTalk Routing . . . . . 15-1***

Overview . . . . . 15-1
Implementation . . . . . 15-1
What is AppleTalk Routing? . . . . . 15-1
Need for AppleTalk Routing . . . . . 15-3
Configuring AppleTalk Routing . . . . . 15-3
Enabling AppleTalk Global Routing . . . . . 15-4
Creating an AppleTalk Routing Interface . . . . . 15-5
Editing AppleTalk Interfaces . . . . . 15-8
Deleting an AppleTalk Interface . . . . . 15-10
Creating an AppleTalk Static Route. . . . . 15-11
Editing AppleTalk Static Routes . . . . . 15-13
Deleting an AppleTalk Static Route. . . . . 15-15
Creating an AppleTalk Name-Binding Protocol (NBP) Filter15-16
Editing an AppleTalk NBP Filter . . . . . 15-18
Adding or Deleting Interfaces to an NBP Filter . . . . . 15-19
Creating an AppleTalk Zone Filter. . . . . 15-20
Editing an AppleTalk Zone Filter. . . . . 15-22
Adding or Deleting Interfaces to a Zone Filter . . . . . 15-23
Viewing AppleTalk Statistics. . . . . 15-24
Viewing AppleTalk Global Statistics . . . . . 15-24
Viewing the AppleTalk Interface Statistics Table. . . . . 15-27
Viewing the AppleTalk Route Table . . . . . 15-28
Viewing AppleTalk Route Table Statistics . . . . . 15-30
Viewing the AppleTalk ARP Cache Table . . . . . 15-31
Viewing the AppleTalk Zone Table . . . . . 15-32
Viewing AppleTalk Zone Table Statistics. . . . . 15-33
Viewing the AppleTalk NBP Table. . . . . 15-34

***Chapter 16 — Managing Intelligent Multicasting . . . . . 16-1***

Overview . . . . . 16-1
Introduction . . . . . 16-1
Manually Configured Intelligent Multicasting . . . . . 16-2
Dynamic Intelligent Multicasting . . . . . 16-3
Configuring Intelligent Multicasting . . . . . 16-5
Configuring Global Intelligent Multicasting . . . . . 16-5
Displaying Router Ports. . . . . 16-8
Configuring Static Router Ports. . . . . 16-9
Searching for Intelligent Multicast Sessions . . . . . 16-10
Deleting an Intelligent Multicast Session . . . . . 16-13
Deleting a Multicast Session Client Port . . . . . 16-14

Creating a Static Multicast Session. . . . . 16-15
Deleting Static Multicast Sessions . . . . . 16-17
Creating Static Client Ports . . . . . 16-18
Deleting Static Client Ports. . . . . 16-19
Managing Internet Group Management Protocol (IGMP) Snooping16-20
Enabling IGMP Snooping. . . . . 16-22
Viewing IGMP Snooping Statistics . . . . . 16-22
Managing the Lucent Group Management Protocol (LGMP) Server16-23
Configuring the LGMP Server . . . . . 16-26
Viewing the LGMP Server Statistics. . . . . 16-27
Viewing the LGMP Server Statistics per VLAN . . . . . 16-28
Managing the Lucent Group Management Protocol (LGMP) Client16-30
Enabling the LGMP Client . . . . . 16-32
Viewing LGMP Clients Statistics . . . . . 16-33
Viewing LGMP Clients per VLAN statistics . . . . . 16-34
Managing Cisco Group Management Protocol (CGMP) Snooping16-36
Enabling CGMP Snooping . . . . . 16-36
Viewing CGMP Snooping. . . . . 16-38

***Chapter 17 — Monitoring the Avaya Multiservice Switch. . . . 17-1***

Overview. . . . . 17-1
Interpreting Front Panel LED Displays . . . . . 17-1
Checking Temperature Status and Configuring Thresholds. 17-2
Checking Active Alarms . . . . . 17-5
Viewing the Active Alarm Table . . . . . 17-5
Using the Event Subsystem. . . . . 17-6
Configuring the Protocol Event Log. . . . . 17-7
Viewing the Event and Shutdown Logs. . . . . 17-12
Viewing Event Statistics . . . . . 17-15
Setting Log Size . . . . . 17-16
Configuring Event Notification . . . . . 17-19

***Chapter 18 — Monitoring and Configuring the Forwarding Cache18-1***

Overview. . . . . 18-1
Configuring the Fowarding Cache . . . . . 18-1
Monitoring the Forwarding Cache Statistics. . . . . 18-4
Displaying Frame Fowarding Statistics. . . . . 18-4
Displaying and Searching the L3 Forwarding Cache for an Entry18-6
Displaying the Forwarding Cache . . . . . 18-9

***Chapter 19 — Analyzing Network Performance By Using RMON and Ethernet Statistics . . . . . 19-1***

Overview. . . . . 19-1
Viewing Network Statistics . . . . . 19-1
Setting Up Port Mirroring . . . . . 19-8
Setting Up a Port Mirror on a Switch in Fabric Mode 1. . . . 19-9
Setting Up Port Mirroring on a Switch in Fabric Mode 2 . 19-13

Removing a Fabric Mode 2 Port Mirror . . . . . 19-19
Viewing Information about a Fabric Mode 2 Port Mirror . 19-20
Setting Up a Port Mirror by Using SNMP . . . . . 19-21
Enabling MAC Address Lock and Traps for Unknown Source Addresses 19-23

## Chapter 20 — Managing Buffers and Queues on 50-Series Modules 20-1

Overview . . . . . 20-1
How Queues Work . . . . . 20-1
Managing Buffers and Queues . . . . . 20-2

## Chapter 21 — 80-Series QoS . . . . . 21-1

Overview . . . . . 21-1
Why implement QoS? . . . . . 21-2
How Does QoS Work? . . . . . 21-3
QoS Process for Ingress Traffic. . . . . 21-3
QoS Process for Egress Traffic . . . . . 21-4
Diagram of QoS Process. . . . . 21-6
Classification of Traffic . . . . . 21-7
Default Priority . . . . . 21-7
Classifying Traffic by Layer 2 Characteristics. . . . . 21-8
Classifying Traffic by Layer 3 or Layer 4 Characteristics . . . 21-8
Diffserv . . . . . 21-10
Precedence of Priorities . . . . . 21-11
Supported Number of Queues. . . . . 21-12
Setting the Priority of a Physical Port . . . . . 21-13
Setting a Physical Port to Ignore Tag Priority . . . . . 21-14
Setting the Priority of a MAC Address . . . . . 21-16
Displaying the Priority of a MAC Address. . . . . 21-18
Setting a Physical Port to Use DiffServ . . . . . 21-19
Setting a Physical Port to Mask DiffServ Bits . . . . . 21-20
Assigning a Priority to a DSCP. . . . . 21-21
Displaying the DiffServ Table . . . . . 21-22
Displaying the QoS Settings for a Physical Port. . . . . 21-22
Setting Up an ACL Rule. . . . . 21-23
Setting Up a Default ACL Rule . . . . . 21-30
Displaying ACL Rules . . . . . 21-31
Ingress Policing. . . . . 21-31
Setting Up Policing . . . . . 21-32
Displaying the Policing Settings. . . . . 21-34
Queue-Servicing Algorithms . . . . . 21-35
WFQ . . . . . 21-35
Strict Priority Queueing. . . . . 21-36
CBQ . . . . . 21-37
CBWFQ . . . . . 21-37
Management Traffic . . . . . 21-38

Setting Up WFQ . . . . . 21-39
Setting Up Strict Priority Queueing . . . . . 21-40
Setting Up CBQ . . . . . 21-41
Setting Up CBWFQ . . . . . 21-42
Displaying the Queue-Service Settings . . . . . 21-46
QoS Statistics . . . . . 21-47
Displaying QoS Statistics . . . . . 21-53
Resetting the QoS Statistics . . . . . 21-54
Displaying the Buffer Settings for Egress Queues . . . . . 21-55

***Appendix A — Upgrading the Application Software . . . . . A-1***

Overview . . . . . A-1
Backing Up the Current Software . . . . . A-2
Backing Up the Previous Configuration . . . . . A-3
Downloading Application Software . . . . . A-5
Setting the Startup Image . . . . . A-6
Synchronizing the Active and Standby Supervisor Modules . . . . A-7
Resetting the Active Supervisor . . . . . A-8
Resetting the Standby Supervisor . . . . . A-9
Verifying the Upgrade . . . . . A-10
Upgrading from v4.***x*** to v5.x . . . . . A-10
Upgrading a Switch with Multiple VLANs Statically Bound to Hunt Group Ports . . . . . A-11

***Appendix B — Boot Mode . . . . . B-1***

Accessing BOOT Mode . . . . . B-1
Accessing BOOT Mode During Power Up . . . . . B-1
Accessing BOOT Mode with Corrupted Operational Images . B-1
Password Recovery . . . . . B-2
Downloading New Operational Code . . . . . B-2

***Appendix C — Supported MIB Groups . . . . . C-1***

General Private MIBs . . . . . C-1
IPX Interface MIBs . . . . . C-1
IEEE 802.3 MAU Management . . . . . C-1
IEEE 802.3 Statistics Group . . . . . C-2
Bridge MIB . . . . . C-2
SNMPv2 . . . . . C-2
RMON . . . . . C-2
RMON2 MIB . . . . . C-2
SMON . . . . . C-2
RIP Version 1.0 and 2.0 . . . . . C-2
OSPF Version 2.0 . . . . . C-2
VRRP . . . . . C-3
IGMP . . . . . C-3
IP Interface . . . . . C-3
IP Version 4.0 and Services . . . . . C-3

IP Forwarding/Route Table . . . . . C-4
DVMRP . . . . . C-4
AppleTalk. . . . . C-4
Policy Capability MIB for LDAP . . . . . C-4
Load MIB. . . . . C-4

***Appendix D — FCC Notice . . . . . D-1***

***IndexIndex 1***

# Preface

## Overview of the Contents

This guide provides information and procedures for configuring the Avaya P550R®, P580, P880, and P882 Multiservice switches with various protocols. You can use either the Web Agent or command line interface (CLI) to configure the switches. This guide provides information for both interfaces. The Avaya switches support both layer 2 and layer 3 functionality.

*** Note:** For detailed information about the CLI, refer to *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

This guide is divided in to the following chapters:

- **Chapter 1, Introduction to the Avaya P550R/P580 P880/P882 Multiservice Switch** — Provides an overview of hardware and software used on all four switches.
- **Chapter 2, Initialize and Setup the Avaya P550R/P580/ P880/P882 Multiservice Switch** — Explains how to initially configure all three switches, and create users, configure protocols, manage configuration files, and configure the switches for dial-up networking.
- **Chapter 3, Configuring System Information —** Explains how to view and configure switch information such as system clock settings, and temperature, power, and cooling statistics.
- **Chapter 4, Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping** — Provides detailed information on how to create and configure VLANs, Spanning Tree, Hunt groups, and VTP Snooping on your switch.
- **Chapter 5, Configuring Port Parameters —** Explains how to configure physical port and switch port parameters on your switch.
- **Chapter 6, Managing Address Forward Tables** — Provides information on how to configure and manage the address forwarding tables in your switch.

- **Chapter 7, Configuring Redundancy Options** — Explains how to install, enable and configure redundancy hardware options on your switch.
- **Chapter 8, Configuring Domain Name System (DNS) and Remote Authentication Dial-In User Service (RADIUS) Clients** — Explains how to configure DNS and RADIUS clients on your switch.
- **Chapter 9, Configuring IP Routing** — Explains how to configure your switch for IP routing and interpret IP routing statistics.
- **Chapter 10, Configuring IP Routing Interface Protocol (RIP)** — Explains how to configure IP RIP on your switch.
- **Chapter 11, Configuring the Open Shortest Path First (OSPF) Routing Protocol** — Explains how to configure OSPF routing protocol on your switch. Also provided is information on OSPF statistical displays.
- **Chapter 12, Configuring IPX Routing** — Explains how to configure IPX on your switch.
- **Chapter 13, Configuring IPX RIP Protocol** — Explains how to configure IPX RIP protocol on your switch.
- **Chapter 14, Configuring IPX Service Advertisement Protocol (SAP)** — Explains how to configure IPX SAP on your switch.
- **Chapter 15, Configuring AppleTalk Routing** — Explains how to configure AppleTalk parameters and view AppleTalk statistics.
- **Chapter 16, Managing Intelligent Multicasting** — Explains how to configure and manage intelligent multicast sessions on your switch.
- **Chapter 17, Monitoring the Switch** — Explains how to use the Web Agent to assess your switch's current operational status.
- **Chapter 18, Monitoring and Configuring the Forwarding Cache (L3 Only) —** Explains how to interpret and monitor forwarding operations that occur in the address cache of the multilayer media modules.
- **Chapter 19, Analyzing Network Performance Using RMON and Ethernet Statistics** — Provides information on how to interpret the statistics counter values displayed in your switch.

- **Chapter 20, Tuning Your Switch Performance** — Explains how to use your switch's buffer management features to optimize traffic throughput through the switch fabric.
- **Chapter 21, Quality of Service** — Provides information about QoS and explains how to configure QoS on the switch.
- **Appendix A, Downloading New Operational Code to the Switch** — Explains how to update the operational code on your switch.
- **Appendix B, Boot Mode** — Explains how to use boot mode on the Avaya Multiservice switches.
- **Appendix C, MIB Groups** — Provides information on the supported MIB groups.
- **Appendix D, FCC Notice** — Provides the FCC notice statement.
- **Index**

# Technical Support

To contact Avaya's technical support:

- **From the United States:**

  1-800-237-0016

- **From North America:**

  1-800-242-2121

- **Outside North America:**

  Contact your distributor

# Avaya Technologies Products and Services

Refer to the Avaya World Wide Web site at:

**http://support.avaya.com**

for information about Avaya products and services.

# Conventions

The following conventions are used throughout this guide

:

| Convention | Represents | Examples |
|---|---|---|
| User Input | User entered text. | To create a new password, type **store password root**. |
| Boldface Text | Represents a menu command, a keyword to be acted upon, or a button name. | In the **Interface** field, select **Default**.<br>Click **Cancel** to stop the installation. |
| System Output | Text displayed by the system. | If you attempt to find the physical location of port 30, the system displays `Unit 2 Port 2` |
| "Save the running configuration to the startup configuration" | Always save the running configuration to startup configuration before you turn off the switch<br>**Note:** Never save the startup configuration to the running configuration. | "Save the running configuration to the startup configuration and turn off the switch". |
| + or - | Expand or collapse a folder in the navigation pane. | To set your server location, you must first expand the System folder, then expand the Configuration folder to see the Server Location link. |
| Using the Web Agent. | The Web Agent consists of folders that you must open to perform a specific operation. The folders are part of a group located on the Web Agent window. | Select **Modules & Ports** from the **System>Configuration** group on the Web Agent window. |
| | | ***1 of 2*** |

| Convention | Represents | Examples |
|---|---|---|
| The words *Select* and *Click*. | In this guide:<br>*Select* means to point and click on a specific item that that opens another dialog box, window, option box, etc.<br>*Click* means to point to an action and press the left mouse button once to perform an operation. | Select **Configuration** from the **Module & Ports** folder. The Module Information Web page displays.<br>Click **Apply** to accept the change, or **Cancel** to ignore the change |
| Web Agent vs. Command Line Interface (CLI) steps. | The procedures in this guide provide detailed steps for the Web Agent. A series of CLI commands are also available that accomplish the same actions. These commands are listed after the Web Agent procedure and are followed by a reference to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for more detailed information. | In the **Ports** field, select the port number of the module.<br>The CLI command is **show port (mod-num>** (refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for more detailed information). |
| Knowledge level | All procedures in this guide are written with the assumption that the reader knows how to navigate through a windows-type environment (use scroll bars, open pull-down menus, etc.). | Scroll to the “Configuring IP by Using the Web Agent” section.<br>Open the **In-band IPC** pull-down menu. |
| | | ***2 of 2*** |

## Using Notes, Cautions, and Warnings

The following text and icon conventions are used in this guide for Notes, Cautions, and Warnings.

*** Note:** Provides additional information about a procedure or topic.

**WARNING**

Indicates a condition that *may cause* bodily injury or death.

**CAUTION**

Indicates a condition that *may damage* hardware or software.

# Related Documentation

This section provides information on the related documentation that supports the Avaya Multiservice switches. This includes:

- Online Documentation and Help Files
- Glossary of Terms

## Online Documentation

Avaya Technologies maintains copies of technical documentation on the corporate Web server. To access online documentation, including HTML and PDF documents, use Netscape Navigator® version 4.5 or higher or Microsoft® Internet Explorer version 3.x or higher and enter the following URL:

**http://support.avaya.com**

## Online Help

You must have a browser installed on your system in order to use the on-line help.

*** Note:** If you are using Netscape®, use version 4.5 or later. Also, you must configure the Proxies to:

**Direct Connection to the Internet**.

Open:

**Edit** > **Preferences** > **Advanced** > **Proxies**

and verify that the **Direct Connection to the Internet** button is selected.

When launching the online help, wait until the help window has completely loaded before resizing the window.

## Installing Online Documentation and Help Files

You can access Online documentation and help files used by the Web Agent by either:

- Installing the HTTP documentation server (available on the Avaya user documentation CD, AvayaDocs)
- Adding the files to an existing web server on your network

You must set up the HTTP documentation help server for the switch. This allows the switch to access:

- Online documentation
- Bitmaps used as part of the interface (logo, wallpaper)
- Online help files for the Web Agent

### Installing the HTTP Documentation Server

You can access online documentation and help files directly from the HTTP documentation server. The server must be running a Win32 compatible operating system (for example, Windows 95, Windows 98, or Windows NT).

To install the HTTP documentation server:

- Run the **Setup** program from the DocsCD CD-ROM

  Or

- Go to the Avaya Product web site:

  **www.avaya.com/support**.

  - Click on **Lan and Backbone Switches**.
  - Click on **P882/P580 Multiservice Switch**
  - Click on **Technical Documentation** from the left pane.
  - Select the **DocsCD**.
- Select the latest released version of the DocsCD.
- Run the **Setup** program (setup.exe). This extracts the help server and the online help system.

## Starting the HTTP Web Server

To run the HTTP help server:

1. Open your system's (Wind32/NT) Start Menu.
2. Select the **DocsCD** program group.
3. Select the document server from that program group.

The Avaya document server will launch. To access this server from a Web browser you need to set a server location on the switch, as explained in "Entering the Server Location on the Switch" section.

## Entering the Server Location on the Switch

To set the location of the documentation server:

1. Launch your Web browser and connect to your switch.
2. Enter your **user name** and **password** at their respective prompts and select OK.
3. Select **Online Help** from the **System>Configuration** group on the Web Agent window. The **Online Help Configuration** page displays.
4. Enter the **host name** or **IP address** followed by the port designation of *:2010* for the HTTP server in the **HTTP Server Location** field (for example, the correct syntax for host named phantom is: `http://phantom:2010`).

*** Note:** If you decide to install your online help on a Web server other than the HTTP server bundled on the DocsCD CD-ROM, you can specify the URL without a port number if your Web server runs on port 80 (for example, `http://www.abc-company.com`).

5. Select **Apply** to accept the server location you entered or cancel to ignore the location.

## Adding Document Files to an Existing Server

You can install the online help to a Web server other than the HTTP server bundled on the DocsCD CD-ROM. You must transfer the help subdirectory to that Web server and enter the URL for that web server in the **Server Location** field.

To transfer the DocsCD help directory to your company server (http://www.abc-company.com):

1. Install the online help and documentation from the DocsCD CD to a Windows95 or NT host on your network.
2. Transfer the entire help subdirectory located in **C:\DocsCD** to the root directory of your Web server.
3. Launch your web browser and connect to your switch.
4. Enter your **user name** and **password** at the respective prompts and select OK.
5. Select **Online Help** from the **System Configuration** folder. The **Online Help Configuration** page displays.
6. Enter the **server location** in the **HTTP Server Location** field (for example, http://www.abc-company.com).
7. Enter the **directory name** of your help files in the **HELP Directory Location** field. For example, **help**.

*** Note:** The default for the help directory is **help**. You do not need to change this unless you changed the name of your help directory.

8. Select **Apply** to accept the HTTP Server Location you entered or cancel to ignore the location.

### Downloading an Updated DocsCD CD from the Internet

The server and help files are available on the Internet. To download updated files from the Internet to your DocsCD CD directory:

1. Launch a web browser.
2. Go to the docs Web page at:

   **http://support.avaya.com**
3. Select the **Lan and Backbone Switchin**g section.
4. Select your product from the product list.
5. Select **Technical Documentation** from the group in the left hand margin.
6. Select the DocsCD zip file for v5.3.
7. Download the DocsCD zip file to the directory you previously created.

For more information on this product, refer to the online documentation that comes on your DocsCD CD-ROM or refer to http://pubs.Avayactc.com to review the online documentation there.

## Documentation

The following documents provide additional information on Avaya products:

- *Avaya P550R, P580, P880, P882 Multiservice Switch Installation Guide, Version 5.3.1* describes how to install and set up the family of Avaya Multiservice switches.
- *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* gives details and command syntax for using the Command Line Interface.

## Terminology

Throughout this guide, the term **Layer 2**, is used to indicate switching capabilities. For example, **Layer 2 Module,** defines a module that enables switching.

The term **Layer 3** refers to the combined ability to switch and route. For example, the name, **Layer 3 module,** defines a module that provides switching and routing capabilities.

# Documentation Feedback

If you have comments about the technical accuracy or general quality of this document please send an email to:

*lsg-CTechpubs@Avayactc.com

Please cite the document title, part number (if applicable), and page reference.

# 1 Introduction

## Overview

The following information is provided in this chapter:


- Switch Descriptions
- Hardware Components
- Software Features
- Routing Overview


## Switch Descriptions

The Avaya P550R, P580, P880, and P882 Multiservice switches are high performance Gigabit Ethernet switches for LAN backbone applications. These switches are the centerpiece for Avaya data, voice, and multimedia LANs. The P550R and P580 switching capacity ranges from 46Gbps in Fabric mode 1 to 55Gbps in Fabric mode 2. The P880 and P882 switching capacity ranges from 56Gbps, in Fabric mode 1, to 139Gbps, in Fabric mode 2.

The Avaya Multiservice switch family supports specific hardware components and various software features, including:

- Increased bandwidth
- Elimination of bottlenecks
- Better manageability
- Routing
- Dependable multimedia support
- Redundant switch-to-switch trunks (or *hunt groups*)
- Enhanced ability to manage user accounts.

# Hardware Components

The Avaya Multiservice switch includes the following hardware components:

## Chassis

The Avaya switch chassis comes in four models:

- The P550R and P580 chassis
- The P880 and P882 chassis.

The P580 and P882 chassis can run in two modes:

- Fabric Mode 1 = 55MHz or Fabric_mode 1
- Fabric Mode 2 = 66Mhz or Fabric_mode 2

### Fabric Mode 1

Fabric mode 1 has a switching fabric performance of 1.76 Gigabits per second per fabric port. Fabric mode 1 modules operate at 55MHz only. The presence of any 50-series modules within the chassis will cause the chassis to operate in Fabric mode 1. P550R and P880 operate only in Fabric Mode 1.

In Fabric mode 1 the P550R/P580 chassis will have a 13x13 crossbar switching fabric, while the P880/P882 chassis will have a 16x16 cross bar switching fabric. In addition, the P880/P882 chassis is limited to sixteen functional slots in this mode (slot 17 can not be used).

### Fabric Mode 2

The 80-series platform is an evolution of the 50-series architecture. It offers a 20% increase in switching fabric performance or 2.11 Gigabits per second per fabric port. This allows greater 10/100/1000 port density on a per crossbar port basis.

This increase in performance is accomplished with Avaya Application-Specific Integrated Circuits (ASICs) that operate at 66MHz (as well as 55MHz capable) and consolidates and enriches the functionality of a number of ASICs used in the 50-series modules.

This increased performance can only occur if the entire switch contains 80-series modules. The presence of any 50-series modules within the chassis will cause the chassis to operate in Fabric mode 1 (they will not power up in Fabric_mode 2).

In Fabric mode 2, the P580 chassis will have a 13x13 crossbar switching fabric, while the P882 chassis will have a 33x33 cross bar switching fabric. All 17 slots in the P882 chassis can be used in Fabric 2 mode.

# Avaya P550R and P580 Multiservice Switch Chassis

The Avaya P550R/P580 Multiservice Switch chassis consists of:

- Seven slots (1 slot for the supervisor module and six payload slots for media modules)
- Fan Tray
- Up to three power supplies
- A 13x13 crossbar switch fabric

## Slots

There are seven slots in the P550R/P580 chassis. Slot 1 is dedicated for a supervisor module and the remaining six are payload slots. If a redundant supervisor is used in the chassis, it must be inserted in slot 2.

## Ports

The P550R/P580 chassis configured with 50-series modules provides support for:

- Up to 120 10/100BASE-TX ports (RJ-45 connector, autosensing)
- Up to 288 10/100BASE-TX ports (Telco connector, autosensing)
- Up to 60 100BASE-FX ports
- Up to 24 gigabit-speed Ethernet ports

The P550R/P580 chassis configured with 80-series modules provides support for:

- Up to 144 10/100BASE-TX ports (RJ-45 connector, autosensing)
- Up to 288 10/100BASE-TX ports (Telco connector, autosensing)
- Up to 144 100BASE-FX ports (MT-RJ connector)
- Up to 48 gigabit-speed Ethernet ports

## Fan Tray

There are two fan assemblies in the chassis. One fan assembly is located on the left side of the chassis to provide air flow to the media modules. This fan assembly is hot-swappable. The other fan assembly is located in the rear of the chassis to provide air flow to the switch fabric. This fan assembly is not field replaceable.

## Power Supplies

Only two power supplies are required to operate a fully-loaded P550R/P580 chassis. A third power supply can be installed to provide backup should one of the other two fail.

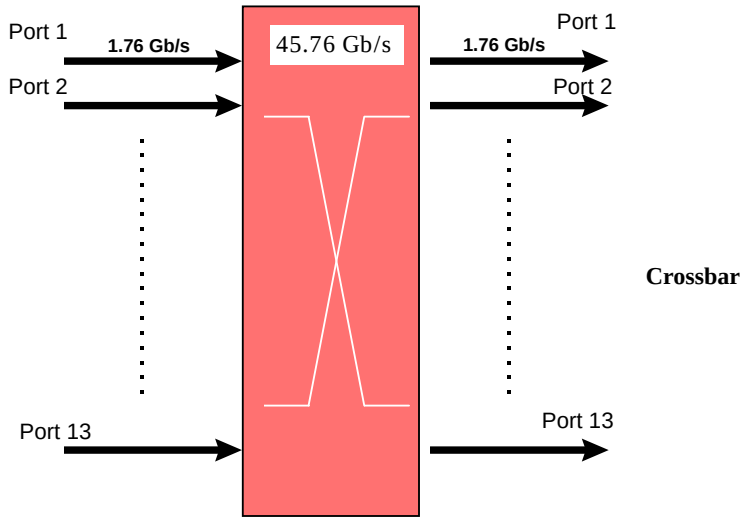
The power subsystem provides N+1 power supply redundancy. In addition, the installed power supplies will load share between the installed units. The power supplies are also warm swappable (power supplies must be turned off and unplugged before removing them from the chassis, however the other power supplies can remain on) The P580 chassis supports both AC and DC power supplies. The P550R chassis supports only AC power supplies.

## Switch Fabric

In Fabric mode 1 (P550R and P580), the switching fabric provides 45.76 Gbps aggregate bandwidth. In Fabric mode 2 (P580 only), the switching fabric provides 54.91 Gbps aggregate bandwidth.

The crossbar switch matrix provides low latency, high throughput packet switching using a crossbar architecture (Figure 1-1).

***Figure 1-1. Crossbar Architecture***



The crossbar supports:

- 13 fabric ports (two per I/O module slot, one for the supervisor module).
- 1.76 Gbps (in and out) on each fabric port in 50-series mode and 2.11 Gbps (in and out) on each fabric port in Fabric mode 2.
- 45.76 Gbps backplane capacity in Fabric mode 1 and 54.91 Gbps backplane capacity in Fabric mode 2.
- Under-subscribed switching fabric in most configurations.
- Single copy replication - Input frames destined for multiple output switch ports pass through the crossbar only once and are copied by the crossbar to each destination.
- Hardware-assisted multicast pruning - The switch only forwards to appropriate destination switch ports.

## Avaya P880 and P882 Multiservice Switch Chassis

The Avaya P880/P882 Multiservice Switch Chassis consists of:

- Seventeen slots (1 slot for the supervisor module and sixteen payload slots for media modules)
- Fan Tray
- Up to three power supplies
- A 33x33 crossbar switch fabric (P882 only)

### Slots

The P880/P882 chassis provides seventeen slots. Slot 1 is dedicated for a supervisor module and the remaining sixteen are payload slots.

In Fabric mode 1, the P880/P882 Chassis supports up to 15 payload slots. Slot seventeen is unsupported in Fabric mode 1. In Fabric mode 2, all sixteen payload slots are usable.

If a redundant supervisor is used in the chassis, the redundant supervisor must be installed in slot 2.

### Ports

With 50-Series modules, the P880/P882 Chassis supports:

- Up to 300 10/100BASE-TX ports (RJ-45 connector, autosensing)

- Up to 720 10/100BASE-TX ports (Telco connector, autosensing)
- Up to 150 100BASE-FX ports
- Up to 60 gigabit-speed Ethernet ports

With 80-Series modules, the P880/P882 chassis supports:

- Up to 384 10/100BASE-TX ports (RJ-45 connector, autosensing)
- Up to 768 10/100BASE-TX ports (Telco connector, autosensing)
- Up to 384 100BASE-FX ports (MT-RJ connector)
- Up to 128 gigabit-speed Ethernet ports

## Fan Tray

There are two fan assemblies in the chassis. One fan assembly is located on the left side of the chassis to provide air flow to the media modules. The other fan assembly is located in the rear of the chassis to provide air flow to the switch fabric. Both fan assemblies are hot-swappable and field replaceable.

## Power Supplies

Only two power supplies are required to operate a fully-loaded P880/P882 Chassis. A third power supply can be installed to provide backup should one of the other two fail.

The power subsystem provides N+1 power supply redundancy. In addition, the installed power supplies will load share between the installed units. The power supplies are also warm swappable (power supplies must be turned off and unplugged before removing them from the chassis, however the other power supplies can remain on). The P882 chassis supports both AC and DC power supplies. The P880 chassis supports only AC power supplies.

## Switch Fabric

In Fabric mode 1 (P880 and P882), the switching fabric provides a 16x16 crossbar with 56.32 Gbps aggregate bandwidth. In Fabric mode 2 (P882 only), the switching fabric provides a 33x33 crossbar with 139.392 Gbps aggregate bandwidth.

The crossbar switch matrix provides low latency, high throughput packet switching using a crossbar architecture.

The Avaya P880/P882 Multiservice switch chassis crossbar supports:

- 33 fabric ports (two per I/O module slot, plus one for the supervisor module - Fabric mode 2).
- 1.76 Gb/s (in and out) on each fabric port in Fabric mode 1 and 2.11 Gb/s (in and out) on each fabric port in Fabric mode 2.
- 56.32 Gb/s backplane capacity in Fabric mode 1 and 139.392 Gb/s backplane capacity in Fabric mode 2.
- Under-subscribed switching fabric in most configurations.
- Single copy replication - Input frames destined for multiple output switch ports pass through the crossbar only once and are copied by the crossbar to each destination.
- Hardware-assisted multicast pruning - The switch only forwards to appropriate destination switch ports

## 50-Series Modules

The Avaya P550R/P580/P880/P882 Multiservice switches support the following 50-Series modules:

- Layer 3 Supervisor Module
- Layer 2 and Layer 3 Fast Ethernet Modules
- Layer 2 and Layer 3 Gigabit Modules
- ATM Uplink Module

The layer 2 and layer 3 media modules implement wire speed routing and bridging in ASICs. The routing and bridging ASICs can process 1.5 million packets per second of minimum-sized Ethernet frames.

*** Note:** All layer 3 modules interoperate with layer 2 modules.

Layer 3 supervisor modules are responsible for learning addresses, and managing the address cache and the Spanning Tree Protocol (STP), as well as other management functions.

The ATM Uplink module provides LAN Emulation (LANE) connectivity over an ATM network.

## Layer 3 Supervisor Module

Layer 3 Supervisor module is part of the path that some packets take through the system.

The 50-Series layer 3 supervisor modules features are:

- PowerPC 750 (RISC) processor
- Memory: 4 MB Flash, 64 MB DRAM, 128 KB NVRAM, 512 KB cache
- Multiple memory configurations (refer to Table 1-1)

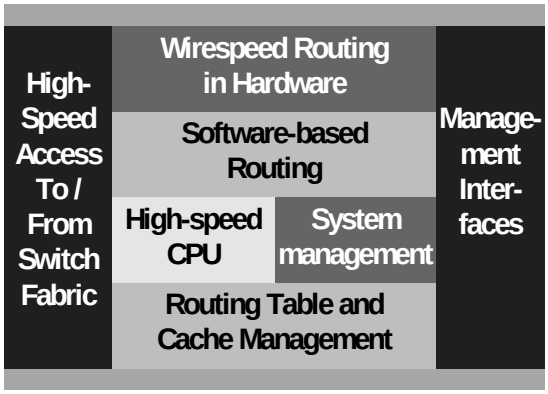
***Table 1-1. Multiple Memory Configuration***

| DIMM/ SIMM | Number of Modules | Total Memory |
|---|---|---|
| 32 MB | 1 | 32 MB |
| 32 MB | 2 | 64 MB |
| 64 MB | 1 | 64 MB |
| 64 MB | 2 | 128 MB |

- Real-time clock
- Out-of-band console: 10/100BASE-T & RS-232
- RMON support
- Simple Network Management Protocol (SNMP) support
- Dot matrix display
- System management functions and interfaces
- Routing protocols tables and caches
- 1.5 million packets per second of hardware-based routing for packets that arrive on layer 2-only media modules
- Software-based routing for packets that are not routed in hardware
- Implementation of layer 3 data forwarding for protocols, such as AppleTalk, that are not implemented in hardware

Figure 1-2 illustrates a conceptual diagram of the layer 3 supervisor module's functions.

*Figure 1-2. Layer 3 Supervisor Conceptual Operation*




Multilayer Supervisor Conceptual Diagram

## Redundant Supervisor

The redundant supervisor module is an auxiliary (standby) supervisor module that acts as a fault-tolerant supervisor in the event that the active supervisor fails. The redundant supervisor provides a seamless solution to switch failure. Once the redundant supervisor is installed, loaded with the same software version as the active supervisor, and synchronized, it is ready to act as a backup to the active supervisor. If the active supervisor does fail, the redundant module quickly assumes control with the least possible effect on network operation. No user intervention is required for the CPU module switchover. The management view is accessible without changing IP or MAC addresses.

The redundant supervisor introduces the concepts of an internal network and internal network mask.

The internal IP network consists of an internal network Virtual LAN (VLAN) that is only used to connect the redundant supervisors in slots 1 and 2. Health messages get passed and image and configuration synchronization access between the supervisor modules are done over the internal IP network. The internal IP network uses the internal network IP mask.

# Media Modules

All of the *layer 3 media modules* have the same general function as the layer 3 supervisor module except for the following:

- The number and type of physical interfaces
- Hardware-based routing and bridging capacity

Bridging and routing are performed on the input side of each media module. Frames whose destination Media Access Control (MAC) address is on the same Virtual LAN (VLAN) as the interface on which they arrived are bridged. Frames that are going from one VLAN to another are routed. Some frames are both bridged and routed, as is the case with multicast.

The media modules' features include:

- **IEEE 802.3x full-duplex flow control -** This allows the switch ports to send a pause command before input buffers overflow. Half-duplex ports support active backpressure (jamming).
- **VLAN trunking or non-tagged access modes -** This allows the switch ports to interoperate with popular tagged trunking schemes used by other vendors.
- **Priority Queuing and Class of Service -** These features allow you to prioritize traffic between particular stations or sets of stations to support jitter-sensitive applications. Supported class of service (CoS) types include the following:
  - 3COM PACE CoS
  - IEEE 802.1p CoS
  - Layer 3 tagging

## Layer 2 and Layer 3 Fast Ethernet Modules

The Avaya P550R, P580, P880, P882 Multiservice switches support the following 50-Series layer 2 and layer 3 Fast Ethernet modules:

*** Note:** HDX stands for Half Duplex, FDX stands for Full Duplex.

- 20-Port 10/100BASE-TX Ethernet module (layer 2 support), with 20 RJ-45 Ports – 10/100, HDX/FDX 100m (M5520-100TX)
- 10-Port 100BASE-FX Ethernet module (layer 2 support), with 10 Fast Ethernet Ports – Fiber, 1300 nM, HDX/FDX multimode fiber, 2Km, SC connectors (M5510-100FX)

- 48-Port, 10/100BASE-TX Ethernet module (layer 2 support), with 4 RJ-21 Telco Connectors – 10/100, HDX/FDX, 100M (M5548N-100TC)
- 10-Port 100BASE-FX Ethernet module (layer 2 and layer 3 support), with 10 Fast Ethernet Ports – Fiber, 1300 nM, HDX/FDX, multimode fiber, 2 Km, SC connectors (M5510R-100FX)
- 12-Port 10/100BASE-TX Ethernet module (layer 2 and layer 3 support), with 12 RJ-45 Ports – 10/100, HDX/FDX, 100m (M5512R-100TX)

## Layer 2 and Layer 3 Gigabit Modules

The Avaya P550R/P580/P880/P882 Multiservice switches support the following 50-Series layer 2 and layer 3 Gigabit Ethernet modules, all with SC connectors.

- 2-Port, Full-Duplex 1000BASE-SX module (layer 2 support) 550M, 850 nM optics, multimode fiber (M5502-1000SX-F)
- 2-Port, Full-Duplex 1000BASE-LX module (layer 2 support) 1310 nM optics, 5Km, singlemode fiber (M5502-1000LX-F)
- 2-Port, Full-Duplex 1000BASE-SLX module (layer 2 support) 10 Km, 1310nM optics, singlemode fiber (M5502-1000SLX-F)
- 4-Port, Full-Duplex 1000BASE-SX module (layer 2 support) 550m, 850 nM optics, multimode fiber (M5504-1000SX-F)
- 4 port, 1310nM optics, 5Km (M5504-1000LX-F) 4 port LX module, singlemode fiber (layer 2 support)
- 4 port, 1310nM optics, 10Km (M5504-1000SLX-F) 4 port SLX module, singlemode fiber (layer 2 support)
- 2-Port, Full-Duplex 1000BASE-SX module (layer 2 and layer 3 support) 550m, 850 nM optics, multimode fiber (M5502R-1000SX-F)
- 2-Port, Full-Duplex 1000BASE-LX module (layer 2 and layer 3 support) 1310 nM optics, 5Km, singlemode fiber (M5502R-1000LX-F)
- 2 port, 1310nM optics, 10Km (M5502R - 1000SLX-F) SLX module, singlemode fiber (layer 2 and layer 3 support)

*** Note:** 802.1p packets that are received with a tag priority of 0 on a 50 series L2 (non-routing) module, but which must be routed via the FORE path on an 80 series supervisor, will be queued and transmitted with a priority of 4. Refer to the "Routing with Layer 2 and Layer 3 Modules" section later in this chapter for more information. This is due to the conversion from the high/low priority system that is used on 50 series modules to the 8-level priority system that is used on 80 series modules.

## ATM Uplink Module

There are four variations of the ATM Uplink module:

- 2 port Synchronous Optical NETwork (SONET)/ Synchronous Digital Hierarchy (SDH) OC-3c/STM-1 Single Mode Fiber (SMF)
- 2 port SONET/SDH OC-3c/STM-1 MMF (MultiMode Fiber)
- 2 port SONET/SDH OC-12c/STM-4c SMF
- 2 port SONET/SDH OC-12c/STM-4c MMF

Each module has two physical interfaces that are capable of being active simultaneously.

The major features of the ATM Uplink module are:

- LANE V2 Client - with LANE 1 compatibility, supports 128 interfaces
- QoS (Quality of Service) support for UBR, nrt-VBR, rt-VBR, and CBR
- ATM UNI (User-to-Network Interface) V 3.0, 3.1 and 4.0 signaling
- RFC 1483 support
- ILMI (Integrated Local Management Interface) Version 4.0
- PNNI (Private Network - to - Network Interface) non-transit
- Link Failover
- Spanning Tree

*** Note:** All ATM protocols are ATM Forum standard.

Refer to the *Avaya P550/P550R Switch ATM Uplink Configuration Guide* for more detailed information.

# 80-Series Modules

The Avaya P550R/P580/P880/P882 Multiservice switches support the following 80-Series modules:

- 4-port, Gigabit Interface Card (GBIC) based module — This module can be configured with up to 4 GBIC optical modules and the GBIC optical modules can support the following distances:
  - 850 nM for multimode fiber (1000BASE-SX) — 550M (50 micron only)
  - 1310 nM for singlemode fiber (1000BASE-LX) — 10Km
  - 1550 nM for singlemode fiber (1000BASE-LX, non-standard) — 80Km

*** Note:** If you use the 1000BASE-SX GBIC with single mode fiber, you must use mode conditioning patch cords with a maximum distance of 500m.

- 8-port, GBIC based module — This module can be configured with up to 8 GBIC optical modules.

  The 8-port GBIC module can support the following GBIC-type connectors:
  - 850 nM for multimode fiber (1000BASE-SX) — 550M (50 micron only)
  - 1310 nM for singlemode fiber (1000BASE-LX) — 10Km
  - 1550 nM for singlemode fiber (1000BASE-LX, non-standard) — 80Km

  *** Note:** If you use the 1000BASE-SX GBIC with single mode fiber, you must use mode conditioning patch cords with a maximum distance of 500m.

- 24-Port 10/100BASE-TX Ethernet module (layer 2 and layer 3 support), with 24 RJ-45 Ports – 10/100, Half Duplex (HDX)/Full Duplex (FDX) (M8024R-100TX)
- 24-Port 100BASE-FX Ethernet module (layer 2 and layer 3 support), with 24 MT-RJ ports multimode fiber, 2Km (M8024R-100FX)
- 48-Port 10/100BASE-TX Ethernet module (layer 2 and layer 3 support), with 4 RJ-21 Telco connectors - 10/100, HDX/FDX, 100M (M8048R-100TC)

- 4-Port 1000BASE-T Ethernet module (layer 2 and layer 3 support), with 4 RJ-45 ports, 100M (M8004R-1000T)
- 8-Port 1000BASE-T Ethernet module (layer 2 and layer 3 support), with 8 RJ-45 ports, 100M (M8008R-1000T)
- Layer 3 Supervisor Module with PCMCIA slot.

*** Note:** When a port on an 80-Series Gigabit Ethernet module is disabled, the port link light blinks continuously. In versions earlier than v5.2.10, the link light extinguished when the port was disabled.

# Software Features

The Avaya P550R/P580/P880/P882 Multiservice switches support the following software features:

- Virtual Bridging Functions
- Flood Pruning Using VLANs
- Hunt Groups
- OpenTrunk Technology
- Three Spanning Tree Modes
- Buffer and Queue Management

## Virtual Bridging Functions

All multiservice switches are designed to support:

- Up to 28,000 MAC addresses in the switch address forwarding table — allows the switch to store forwarding information for hosts in very large networks.
- Segmented address tables qualified by address and VLAN membership — allows the same host to appear on different VLANs on different ports.
- Optional per-VLAN Spanning Tree Protocol — isolates loop control to smaller domains, so spanning trees converge faster after a topology change.

# Flood Pruning Using VLANs

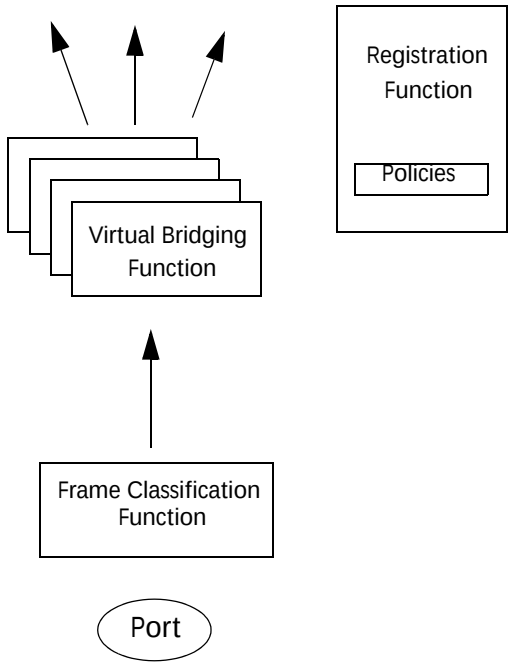
VLANs provide network managers with two significant capabilities:

- The ability to segment traffic in a flat switched network. This helps prevent traffic from being forwarded to stations where it is not needed.
- The ability to ignore physical switch locations when creating workgroups. VLANs are logical constructions and can traverse physical switch boundaries.

The hardware on all multiservice switches support port-based VLANs with the following characteristics:

- Frames classified as Layer 1 (Port-based) when they enter the switch
- Explicitly tagged VLAN packets — these are forwarded based on the information in the packet.
- Up to 1,000 VLANs — VLANs define a set of ports in a flooding domain. Packets that need to be flooded are sent only to ports participating in that VLAN (Figure 1-3).

***Figure 1-3. Flooding Domain***



## Hunt Groups

Hunt groups allow you to aggregate bandwidth from multiple ports so they act as one high-bandwidth switch port. Hunt groups create multi-gigabit pipes to transport traffic through the highest traffic areas of your network. You can create hunt groups that interoperate with other vendors' equipment (for example, Cisco's Etherchannel and Sun's Quad Adapter).

## OpenTrunk Technology

The Avaya P550R/P580/P880/P882 Multiservice switches are delivered as a plug-and-play IEEE 802.1D standard bridge, but support several VLAN tagging schemes. This makes the switch highly interoperable in existing networks because:

- Any port can be a trunk port.
- Ports have configurable VLAN tagging on a per-port basis.
- Ports process a number of popular VLAN tagging schemes, including major vendors' proprietary schemes.

The following are features of Open Trunk Technology:

- Frame encapsulation
  - Identifies frame VLAN via tag
  - Associates frame priority
- Multiple tagging formats
  - IEEE 802.1Q
  - A major vendor's multi-level tagging scheme
  - 3Com VLAN Tag & PACE priority signalling
- Translation to and from any format. A packet can enter the switch with a 3Com SuperStack II VLAN tag and exit the switch as a multi-layer tagged packet.

## Load MIB

The switch Load MIB defines upload, download and copy of application software and configuration information. The Load MIB consists of two tables:

- The genOpTable — a conceptual table where each row represents a file operation that can be performed by the switch. For example, `localConfigFileCopy` is a function that the switch software supports. Therefore, the genOpTable should always display the conceptual row representing the indicated operation.
- The genAppTable — functions as a file system directory. Each row in the genAppTable represents a file stored in ram, nvram, flash, or bootprom. By using this representation, the network management device can walk the entire genAppTable to learn what files (along with their type and location) are resident in the system.

## Spanning Tree Modes

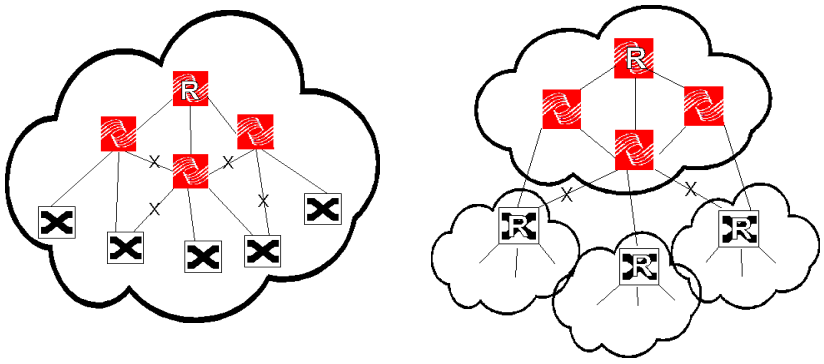
Spanning tree protocol is used to prevent loops from forming in your network. The spanning tree algorithm creates a single path through the network by ensuring that if more than one path exists between two parts of a network, only one of these paths is used, while the others are blocked.

### Spanning Tree Protocol Bridge Options

All multiservice switches support the following four Spanning Tree Protocol options:

- IEEE 802.1D Spanning Tree
- Per-VLAN Spanning Tree
- Dual-Layer Spanning Tree (Figure 1-4)
- Global Disable

*Figure 1-4. Spanning Tree Models*



Single 802.1D Spanning Tree
One Spanning Tree
Longer convergence
One path to and from root for all VLANs
Improper configuration
can shut down Trunk Links

Multi-Level Spanning Tree
Backbone terminates 802.1D STP
Smaller STP Domains
Quicker Convergence
VLAN Load Balancing
Interoperates w/ existing Bridge/Routers

## *IEEE802.1D Spanning Tree Protocol Option*

All Avaya Multiservice switches participate in a Single Spanning Tree domain in the IEEE802.1D STP mode. All ports with STP configured belong to the same spanning tree domain and rules are as defined in IEEE802.1D. BPDUs are as defined by 802.1D and are sent out Clear on each link regardless of whether or not the link has a tagging method defined. As documented in the IEEE specification, 802.1 D Spanning Tree is intended for environments where only one VLAN is used in the network. If you are using 802.1 D Spanning Tree in the network and have multiple VLANs, you should set the P550R, P580, P880, or P882 switches to run Dual-Layer Spanning Tree.

## *PER VLAN Spanning Tree Protocol Option*

Per-VLAN mode is the Default Spanning Tree setting on all multiservice switches. In this mode, the switch runs a separate spanning process for each VLAN. Each logical Spanning Tree has its own BPDU's which are tagged with the appropriate VLAN Identifier(s). Under this mode, the switch can participate in as many Spanning Tree Domains as there are VLANs defined on the switch. This conforms to a “virtual” bridging model where the switch runs as if each VLAN is a separate logical bridge (separate Address Forwarding Tables, separate spanning trees, etc.). If spanning tree is not required on all VLANs, you can disable it for individual VLANs on a VLAN by VLAN basis. Also, different root bridges can be configured with different bridge priorities based upon VLAN. This will allow load sharing to occur based upon VLAN. Similarly link costs and priorities can be adjusted on a per-VLAN basis allowing further load sharing per VLAN.

Per VLAN Spanning Tree is the recommended method whenever many VLANs are passed over interswitch links, but not every VLAN resides on every interswitch link. If IEEE 802.1D Spanning Tree mode is used without care under these constraints, VLANs can be split due to blocking on inappropriate links. The only time that Per-VLAN mode may become undesirable is when you have more VLANs to manage than the number of Spanning Tree Domains. The only other constraint is to limit the number of outgoing BPDUs.

It is required that the number of outgoing BPDUs be less than 500/second on all multiservice switches. This means that if you have 50 VLANs you cannot have more than 20 possible paths back to the root bridge (50 VLANS X 20 LINKS X 0.5 BPDU/sec. = 500), or if you have 100 VLANs you cannot have more that 10 possible paths back to the root bridge. These constraints are not generally exceeded in real networks. If these limits are exceeded, you must use 802.1D Spanning Tree mode.

This method can easily inter-operate with legacy IEEE802.1D Devices. The legacy devices become part of the VLAN associated with the VLAN port binding with which they are attached. In other words, if there are 3 P550's in a network running VLANA and VLANB, and three legacy devices connect up through a port configured in VLAN A, the legacy devices will become part of the VLAN A Spanning Tree. The P550's will participate in two Spanning Tree domains, one for VLAN A containing three bridges and one for VLAN B containing 6 bridges. The legacy devices need not be VLAN aware.

### *Dual-Layer Spanning Tree Protocol Option*

Dual-Layer spanning tree mode is a variation of per-VLAN spanning tree mode with many of the same features. However, instead of using normal BPDUs, which are clear (free of VLAN tags) on clear links and tagged on tagged links, as is the case with Per-VLAN Spanning Tree mode, dual-layer uses a proprietary BPDU. This proprietary BPDU is sent to a special multicast address and contains information about which VLAN the BPDU is associated with. This has an advantage over per-VLAN spanning trees in that this method can support multiple VLANs over a non-tagging link, or when connecting to a bridge/router.

In this mode, legacy bridges remain in separate Spanning Tree domains, yet loops between the layer 3 and legacy domains cannot form. For example; if there are three P550 multiservice switches in a network running VLAN A and VLAN B, and three legacy devices connect up through a port configured in VLAN A, the legacy devices remain in their own legacy Spanning Tree and do NOT join the Multilayer Spanning Tree.

In the previous example, all three multiservice switches participate in two Spanning Tree domains:

- Domain for VLAN A containing three bridges
- Domain for VLAN B containing three bridges with the legacy domain remaining separate.

The legacy devices need not be aware of the other spanning tree domains. If a loop forms between the Multilayer domains and the legacy domain, the proprietary BPDU is seen returning to the Multilayer domain through the legacy domain and the loop is blocked. The Dual-Layer Spanning Tree method is preferred when inter-operating with large legacy bridge networks. Convergence time is reduced, and management is simplified, by allowing the legacy bridges to remain in their own spanning tree domain

## Global Disable

You can globally disable Spanning Tree on all multiservice switches, thus preventing any switch port from participating in Spanning Tree. This is only recommended in a very controlled environment where there is no possibility of a loop being placed in the network.

### *Port Settings*

You can use the “Bridge Ports” option to adjust link costs and priorities per IEEE802.1D. You can also disable Spanning Tree on a per port basis by a per-port port parameter setting. If you disable Spanning Tree per port, IEEE802.1D definitions are strictly followed. This means that BPDUs are not sent, incoming BPDUs are not processed. You can also set the port to Spanning Tree disable if you do not want that port to “participate”. The port is then put directly into Forwarding State: meaning BPDUs cannot be sent out the port, incoming BPDUs cannot be processed, and received traffic can still be forwarded.

### *Spanning Tree Design*

Avaya recommends that you consider the following standard IEEE802.1D Guidelines when you design your network, no matter which Spanning Tree mode you decide to use:

- Assure core switches can be forced to be root bridges. For per-VLAN Spanning Tree, the function of root bridge can be shared among several core switches
- When using standard timers assure the depth of the tree does not exceed 7 bridges when a default bridge timer is used
- Enable FAST START on all ports that include IPX and DNS clients.

## Extensive Fault Tolerance

All multiservice switches are designed to function as backbone switches. You can install each switch in your network's core without creating a single point of failure.

Extensive fault tolerance features include:

- N+1 power. Power supplies share the power supply load. If one fails, the remaining supplie(s) assume the load automatically and the switch management system warns of the failure.
- Hot-swappable fans and modules - Each fan and module can be changed from the switch front panel, without powering down the switch.
- Redundant switch links (using spanning tree and link aggregation groups).
- Front-loadable cables, modules, power supplies and fans.
- Redundant switch element and switch controller modules (fault-tolerant switches only).

## Buffer and Queue Management

Buffer and queue management relieves congestion in a network. Adding gigabit speeds to existing networks means that there can be a huge disparity between link speeds. For example, anything more than a 1-percent load on a gigabit link could easily overwhelm a 10 Mb/s Ethernet link.

Each switch employs the following buffer and queue management techniques:

- Configurable active backpressure:
  - Half-duplex ports use active backpressure to jam input ports when their frame buffers are full.
  - Full-duplex links use IEEE 802.3z pause control frames to pause traffic when buffers are full.
- Packed frame buffers for optimal memory utilization. The memory management allows virtually 100% utilization of buffer memory.

- Two CoS priority queues for 50-Series modules and eight CoS priority queues for 80-Series modules provide flexible queue management algorithms to meet application requirements.
- Configurable queue depth for each prioritized packet queues.
- Configurable priority threshold.
- Configurable service ratio tunes queue priority.

# New Software Features

## v5.3 Software Features

The following new software features are implemented in Version 5.3:

- Custom Access Types.

  This feature allows you to create custom access types in addition to the standard **READ_ONLY**, **READ_WRITE**, and **ADMINISTRATOR** access types. For information about creating and managing custom access types, see "Configuring Custom Access Types" on page 2-12.

- CLI support for the following Quality of Service (QoS) features:

  — Queue servicing by means of class-based queuing (CBQ).

  — Queue servicing by means of class-based weighted fair queuing (CBWFQ).

  — Policing, which makes it possible for you to limit the bandwidth for ingress traffic and drops frames when traffic exceeds the limit.

  — New CLI commands for setting queue servicing for egress traffic.

  — Ability to view and reset QoS statistics.

  — Ability to view buffer allocation.

  For information on how to set up the QoS features, see Chapter 21, "80-Series QoS."

- Routing-only IP interfaces.

  You can now set an IP interface to route but not allow management of the switch. For information on how to set an IP interface for routing only, see "Creating and Assigning IP Interfaces to the VLAN" on page 9-6.

- Reset individual modules by using a CLI command.

  For information on how to reset an individual module, see "reset-module" in Chapter 17, "Module," of the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

- Debug mode

  This mode displays system messages to help you troubleshoot network problems. Use the **set debug {on | off}** CLI command to enable and disable Debug mode. By default, this mode is disabled.

- Enhanced ability to manage user accounts.

  These enhancements increase the security of the switch and are as follows:

  — The switch administrator is now able to enable or disable the **manuf** and **diag** user accounts, and the switch retains the setting when you restart the switch.

  — Users with administrator access can change their own password and the password of other users, excluding the **manuf** and **diag** accounts. In earlier versions of software, users with administrator access could change the passwords for the **manuf** and **diag** accounts.

  Users without administrator access, excluding the **manuf** and **diag** accounts, cannot change any passwords.

  — Users logged in as **manuf**, **diag**, or **root** can change their own passwords. However, these passwords revert to the default passwords when you initialize NVRAM (NVRAM initialize).

  For information on how to disable the **manuf** and **diag** accounts, see "Disabling User Accounts" on page 2-19.

- Internal Error Detection and Recovery (IEDR)

  This feature shuts down a port if its rate of internal CRC errors exceeds the threshold setting. Currently you can enable this feature only by using the CLI and only for ports

on 50-series and 80-series gigabit modules. For more information about this feature, see "Internal Error Detection and Recovery" on page 5-44.

- MAC address filters for 80-series port mirrors.

  This feature makes it possible for you to set up port mirrors that monitor only traffic with a specific source MAC address or destination MAC address. For information on how to set up Fabric mode 2 port mirrors that use MAC address filters, see "Setting Up Port Mirroring on a Switch in Fabric Mode 2" on page 19-13.

- Support for the following MIB groups and objects:

  — MIB II, documented in RFC 2863

    • Hunt group objects in the ifTable of the Interfaces Group

    • Hunt group objects in the ifXTable of the Interfaces Group

  — Bridge MIB, documented in RFC 1493

    • Dot1dTp Group

    • Dot1dStatic Group

  — RMON MIB, documented in RFC 1757

    • Alarm Group

    • Event Group

  — RMON2 MIB, documented in RFC 2021

    • Trap Destination Table in the Probe Configuration Group

  — RFC 1483 MIB

  — LEC MIB (documented by ATM Forum in specification AF-LANE-0093.000)

# v5.2.10 Software Features

The following software features were implemented in v5.2.10:

- Non-Broadcast Multi-Access (NBMA) IP Interfaces

  This feature makes it possible for the switch to exchange routing information over nonbridged connections (routed virtual switch ports). NBMA functionality has been added to the RIP and OSPF routing protocols in the switch software and has been tested with Cisco and Marconi routers.

  NBMA functionality is being developed in the Avaya Multiservice switch software for the ATM uplink module. This feature makes it possible to set up an IP interface as NBMA. Marconi and Cisco routers use NBMA IP interfaces and neighbor lists to exchange OSPF route updates. For information on how to set up NBMA IP addresses, see "NBMA IP Interfaces" on page 11-33.

- Network Error Detection and Recovery (NEDR)

  This feature monitors Ethernet CRC errors on Ethernet data ports and compares the rate of errors to the threshold setting. If you enable this feature, you can log errors in the Event log and shutdown the port that is receiving the CRC error packets. You can enable this feature only by using the CLI and only for ports on 50-series and 80-series gigabit ethernet modules. For more information about this feature, see "Network Error Detection and Recovery" on page 5-39.

- CLI command to view information about all hardware in the chassis.

  For more information about this feature, see "show module-inventory," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

# v5.2.6 Software Features

The following software features were implemented in v5.2.6:

- The following Queue Classification and Servicing features:
  - Classification of layer 2 traffic by:
    - Source MAC address
    - Destination MAC address
    - Differentiated Services (DiffServ) code point
  - Classification of layer 3 traffic by:
    - Default layer 3 priority (which you set)
    - DiffServ code point
    - Layer 2 priority
  - Mapping of DiffServ code points to priority queues
  - Strict Priority Queue Servicing

  For more information about these Queue Classification and Servicing features, see Chapter 21, "80-Series QoS."
- GBIC Identification.

  This feature identifies the type of gigabit interface converters (GBICs) that are connected to the 80-series, 4-port and 8-port Gigabit modules. For more information about the GBIC identification feature, see "GBIC Identification" on page 5-38.
- SNMP MIB support for port mirroring.

  For more information about using SNMP to perform 80-Series port mirroring, see "Setting Up a Port Mirror by Using SNMP" on page 19-21.
- Ability to set whether Avaya Policy Manager (APM) stops or continues to apply a policy if an error with a command occurs.

  For detailed information about the CLI commands used to set this option, refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

- Ability to reset the switch remotely by using SNMP.

  For more information about using SNMP to reset the switch remotely, see the "Performing a Reset" on page 3-16.

## v5.2.2 Software Features

The following software features were implemented in v5.2.2:

- The following Queue Classification and Queue Servicing features:
  - Classification of switch port traffic.
  - Classification of layer 2 tagging.
  - Classification of layer 3 traffic (by means of an access control list).
  - Queue servicing by means of weighted fair queueing (WFQ).

  For more information about these Queue Classification and Servicing features, see Chapter 21, "80-Series QoS."
- Port mirroring on a switch that is operating in Fabric mode 2.

  This feature makes it possible to:
  - Monitor traffic that is received and transmitted from a port.
  - Use up to four monitor channels for monitoring traffic.

  For more information about port mirroring on a switch that is operating in Fabric mode 2, see "Setting Up Port Mirroring on a Switch in Fabric Mode 2" on page 19-13.

## v5.2.0 Software Features

- Relay Agent Information option (option 82) for Dynamic Host Configuration Protocol (DHCP).

  When forwarding client-originated DHCP packets to a DHCP server, the Avaya multiservice switches insert this option, which contains information about the switch. The DHCP server uses this information to authenticate the client. For more information about option 82, see "Option 82 for DHCP" on page 9-48.

- Enhancement of the MAC Address Lock feature.

  This feature has been available in all previous releases. If a source MAC address is locked at a port (statically configured), a frame with that source MAC will be filtered if received on any other port on the same VLAN. With the enhancement, the feature immediately generates traps to identify all unknown source addresses. If, after sending a trap for an unknown source, the switch continues to receive traffic from the source, the feature generates a trap every 30 minutes until the traffic stops.

  *** Note:** You can set the trap timer within a range of 60 to 1800 seconds (default) in one second intervals.

  For more information about the MAC Address Lock feature and traps for unknown source addresses, see "MAC Address Lock and Traps for Unknown Source Addresses" on page 6-24.

- Load MIB for the ATM Uplink module, V1.1 or later.

  This feature makes it possible for you to use SNMP commands to:

  — Upload the startup configuration file of the ATM Uplink module to a TFTP server

  — Download the startup configuration file from a TFTP server to the ATM Uplink module.

  — Download a software image to the ATM Uplink module.

# Routing Overview

All P550R/P580/P880/P882 Multiservice switches can be configured as an IP, IPX, and AppleTalk router with virtual interfaces. Virtual interfaces are mapped to physical ports or VLANs. Layer 3 IP traffic is routed between the virtual interfaces.

Ports become members of VLANs by being assigned or by rules. Multiple VLANs can share a single trunk port. In contrast, multiple physical ports can be associated with a single VLAN. In all cases, traffic that arrives and leaves the same VLAN is bridged, not routed.

This section provides the following sections:


- Compatibility with Layer 2 Modules
- Routing with Layer 2 and Layer 3 Modules


## Compatibility with Layer 2 Modules

Each switch is completely backward compatible with all of the layer 2 media modules that the switch currently supports. Layer 3traffic is routed by sending that traffic to the layer 3 supervisor module. The supervisor module routes all traffic from layer 2 media modules as described in the next section, "Routing with Layer 2 and Layer 3 Modules."

*** Note:** Layer 2 traffic that does not require routing is bridged independently of the layer 3 traffic based on the MAC address or VLAN information.

## Routing with Layer 2 and Layer 3 Modules

When a switch is configured with a mix of layer 2 and layer 3 modules, IP and IPX routing is performed by the layer 3 media modules or the layer 3 supervisor module using special ASICs present on those modules. These ASICs contain an *address cache* (forwarding table) that can contain a maximum of 20,000 cache entries. The address cache entries consist of packet addressing information and next hop information that enable the switch to effectively route the packets to their destination.

The layer 3 supervisor module also maintains a *master routing table* that is kept in the its memory. The master routing table can contain up to 28,000 entries. This routing table enables the supervisor module to keep track of which entries are in each address cache. As a result, each time a change occurs in the master routing table, the layer 3 supervisor module updates the appropriate address caches. For example, if a unicast route is removed from the master routing table, all matching entries in address caches are also removed.

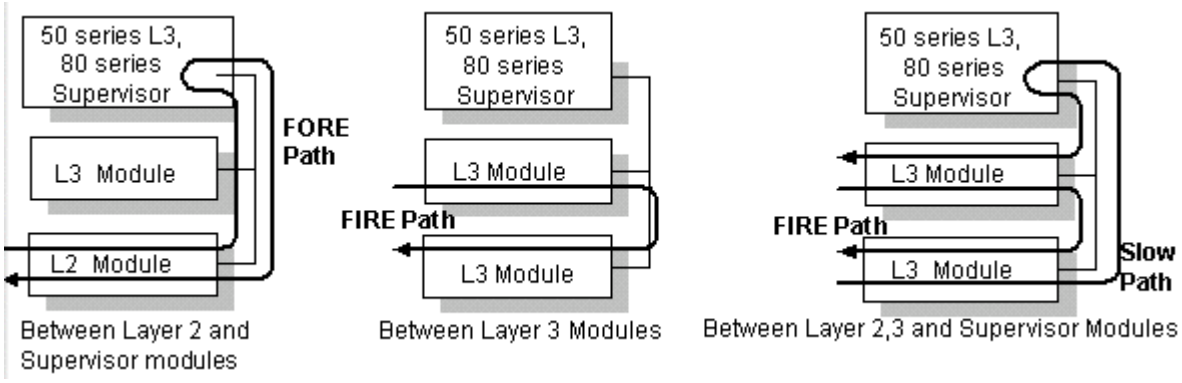
Consequently, when you connect a switch to the network, it begins to receive frames from the network and builds a master routing table (supervisor module) and forwarding tables (address caches of media modules) based on those frames.

This process creates three distinct results:

- All known (learned) layer 3 traffic that requires routing, is routed directly by the 50 series layer 3 or 80 series media module without a need to traverse the switching fabric to get to the supervisor module's software routing function. This is referred to as the **FIRE** path, or Fast Inband Routing Engine, since the routing is accomplished in the hardware in the media modules.
- All unknown (not learned) layer 3 traffic must first be sent to the 50 series layer 3 or 80 series supervisor module, where information on the frame is added to the supervisor module's master routing table, then it is added to the address cache of each applicable layer 3 media module. This is referred to as the **Slow Path**, since the routing is accomplished by the CPU and software in either supervisor module instead of the hardware in the media modules.The **Slow Path** is used when the destination is unknown for IP and IPX packets and for all AppleTalk routing.
- Since layer 2 modules have no routing capability, packets that are received by a layer 2 module and require routing are forwarded by sending the packet to the 50 series layer 3 or 80 series supervisor module. The routing engine on the supervisor module then performs the routing operation for the layer 2 modules and sends the packet back through the switching fabric to the destination port.This is referred to as the **FORE** path, or Fast Out of Bands Routing Engine, since the routing is accomplished in the hardware of either supervisor module.

Figure 1-5 shows how traffic is routed in a switch.

***Figure 1-5. Layer 2 and Layer 3 Routing in a Switch***



# 2 Initialize and Setup

## Overview

The following information and procedures that are provided in this chapter are common to both layer 2 and layer 3 module configuration:

- Setting Up Your Laptop or PC Monitor
- Configuring the Supervisor Module Using the CLI
- Configuring the Switch Using the Web Agent
- Configuring Custom Access Types
- Configuring User Accounts
- Remote Authentication Dial-In User Service (RADIUS) Client Support
- Changing the Console Serial Port Settings
- Configuring Dial-Up Networking
- Changing the TCP Ports for HTTP and Telnet
- Managing Configuration Files

*** Note:** The last step in each procedure tells you to click Apply to save any setup or changes you made. This saves the setup or any changes to the **Running config** only. The **Startup config** has not changed. Therefore, these and other changes will be lost if your switch goes down or if you power it off.

To save these changes to the Startup Config, you must copy the **Running config** to the **Startup config**. Refer to the "Copying Configuration Files" section later in this chapter.

# Setting Up Your Laptop or PC Monitor

You need a laptop or PC to make a serial line connection to the switch to complete initial switch setup. Table 2-1 lists the settings required for the laptop or PC monitor to communicate with the switch.

***Table 2-1. Laptop or PC Monitor Settings***

| Baud Rate | Stop Bits | Data Bits | Flow Control | Parity |
|---|---|---|---|---|
| 9,600 | 1 | 8 | Xon/Xoff | None |

## Managing the Avaya Multiservice Switch using Telnet

There are several ways to manage the Avaya Multiservice switch. In addition to managing the switch via WEB agent, SNMP and serial console CLI commands, the switch provides telnet server capability. Through this Telnet session, an administrator can manage the switch via CLI commands.

### Setting up an Interface

Before you can establish a Telnet session you must configure an IP interface to allow management of the switch. From the IP Interfaces Web page or via CLI command, create an IP Interface and configure the IP Routing option for either Routing/Mgmt or Mgmt. For more information on setting up an IP Interface on the switch, please refer to the *Creating an IP Interface* section in Chapter 9, *Configuring IP Routing*, in the *Avaya Multiservice Switch P550/P880/P882 Switch User Guide*.

### Establishing a Telnet Session

Once an IP Interface has been setup and configured to allow management traffic, you are now ready to open a telnet session to the switch. To do this you will need to use one of the commercially available telnet clients. Launch the telnet client application and open a telnet session with the IP address of the management interface. You will be presented with the switch's login prompt.

If the TCP port for Telnet requests is set to a port number other than 23, you must specify the TCP port number in addition to the IP address or host name to start a Telnet session. For example, if you change the TCP port from 23 to 9998 on switch 192.168.0.126, enter **telnet 192.168.0.126 9998** to start a Telnet session. For information on how to change the TCP port for Telnet requests, see Changing the TCP Ports for HTTP and Telnet (page 43).

Once logged into the switch via telnet session, you can manage the switch using the CLI commands. For more information on CLI commands, see the *Avaya Multiservice Switch P550R/P880/P882 Switch Command Reference Guide*.

The Avaya Multiservice Switch supports a maximum of 6 concurrent telnet sessions. This allows multiple network administrators to connect to and manage the switch. However, if multiple telnet sessions are opened, configurations changes from one session could be overwritten by configuration changes from another.

*** Note:** Avaya recommends that you use one telnet session at a time to manage the switch.

Although it is possible to establish nested telnet sessions, Avaya recommends that you establish a separate telnet session for each switch that you want to manage. A nested telnet session occurs when you establish a telnet session from a client to one switch, then through that session, open another telnet session to a second switch. Having a separate telnet session for each switch that you want to manage will help to avoid confusion.

### Terminating a Telnet session

To terminate the telnet session gracefully, exit the management session by repeatedly typing *exit* until you reach the "Login" prompt. To end the telnet session from the client, enter the client-specific command to terminate the session.

### Troubleshooting Tip

When entering CLI commands in a telnet session, memory is allocated to hold the CLI command history. Closing the telnet session abruptly by terminating the telnet client application does not free this memory and may cause the switch to reset.

Close the Telnet session gracefully as explained in the previous section.

## Viewing Active Telnet Sessions

To view active telnet sessions on the switch enter the **show sessions** command as shown in the example below. A list of active telnet sessions will be displayed.

```
Welcome to the Avaya *Enhanced* CLI

Avaya> show sessions
Session ID    Line ID    Location
*0              9vty
```

```
123.123.123.123:1211
```

## Telnet session expiration timer

Once a telnet session is established, the session will remain open while there is activity. However, if the session is left idle, the session will expire and will be automatically terminated based on the setting of the telnet inactivity-period command. The default setting for this timer is 900 seconds or 15 minutes. Setting this timer to 0 deactivates the inactivity timer so the telnet session will not expire.

You can set the telnet inactivity timer in configure mode as follows:

```
<configure># IP telnet inactivity-period
<time-out in seconds>
```

| | | |
|---|---|---|
| Minimum value: | 0 seconds | Disables inactivity timer |
| Default value: | 900 seconds | Expiration time is 15 minutes. |
| Maximum value: | 65,536 seconds | Expiration time is approx. 18 hrs. |

**CAUTION**

Avaya recommends not to disable the inactivity timer. If the inactivity timer is disabled and the maximum number of telnet sessions are open, none of them will expire. Subsequent attempts to establish a telnet session will fail. Additionally, idle Telnet sessions may represent security risks.

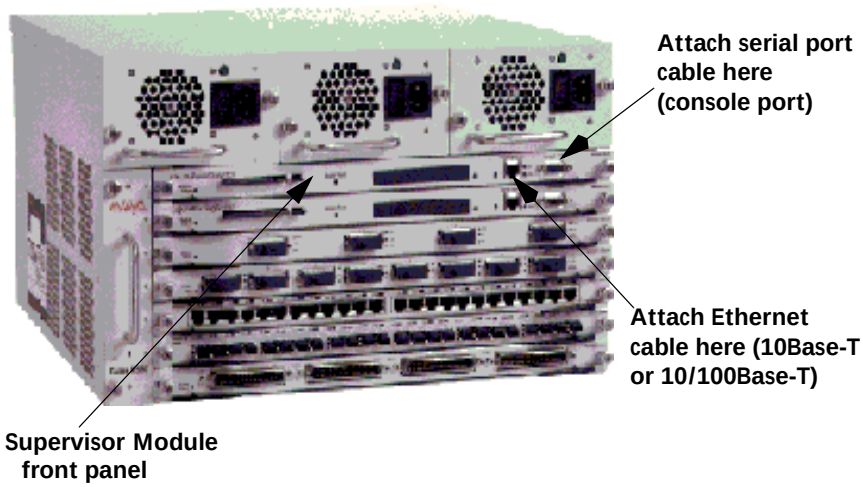
# Configuring the Supervisor Module Using the CLI

To connect to the Web Agent, you must first use the serial command line interface (CLI) to configure the switch's IP address and a subnetwork mask on the supervisor module.

To configure the supervisor module using the CLI:

1. Attach a 9-pin straight-through male-to-female serial cable from the serial port on your laptop or PC to the serial port on the supervisor module's front panel (Figure 2-1).

*Figure 2-1. Avaya P550R/P580 Multiservice Switch Front View*


Attach serial port cable here (console port)
Attach Ethernet cable here (10Base-T or 10/100Base-T)
Supervisor Module front panel

2. Run a terminal emulation program (HyperTerminal, for example) on the attached laptop or PC. Verify that the laptop or PC monitor settings match those listed in Table 2-1.

3. Power up the switch. The switch displays the following startup messages in the terminal emulation program:

```
Booting the operational system, please wait....

Initializing the file subsystem... done
Initializing the event subsystem... done
Initializing the agent subsystem... done
Initializing the platform... done
Initializing the switch subsystem... done

Starting up threads...
    Periodic Task
    Event
    Network Interface
    Switch Interface
    Telnet Processes
    Ping Process
    Module Manager
    Address Table Aging
    Multicast Pruning
    Front Panel Display
    Download
    Fans Poller
    Power Supplies Poller
    VTP Snooping
    Redundant Controller/Element Poller Task
    Command Line Parser
Powering up modules
Module 1 Powered
```

```
Waiting for power cycle to complete (The 17 second power cycle
option)
Module 2 Powered

Initializing the module subsystem... done

System initialization complete.

Configuring system from Startup Config file [/nvram/
startup.txt]... done
Boot process complete - system is now operational.(3.0->4.0
conversion)
Creating Startup Config file [/nvram/startup.txt]... done

Copyright © 2002, All rights reserved by Avaya Incorporated

This software is furnished under a license and may be used in
accordance with the terms of such license and with the
inclusion of the above copyright notice. This software or any
other copies thereof may not be provided or otherwise made
available to any other person.
No title to and ownership of the software is hereby
transferred.
Contains software developed by:
Epilogue Technology Corporation
Copyright (c) 1988 - 1996 Epilogue Technology Corporation
TEC Technically Elite Concepts, Inc.,
Copyright (c) 1994 by Technically Elite Concepts, Inc.,
Hermosa Beach, California, U.S.A.

ISI Integrated Systems, Inc.
Copyright 1991 - 1995, Integrated Systems, Inc.

All other trademarks used herein are the property of their
respective owners.

Avaya Inc. Multiservice Switch Agent v5.3.1
Press Ctrl-P for previous command, Ctrl-N for next command,?
for help.

Login:
```

*** Note:** Login information and Password prompts are case sensitive.

4. Enter **root** at the **Login** prompt. The password prompt displays.

5. Enter **root** at the **Password** prompt. The command line interface prompt displays. You must now change he command mode to the configure mode so that you can use the `setup` command.

6. Complete the following steps to change the command mode to the configure mode:

   a. Enter the `enable` command.

   b. Enter the `configure` command.

7. Enter the `setup` command. This initiates a series of queries. Answer each query as follows:

   a. Press **Enter** when prompted to change the super user password. This accepts the default of **Yes**

   b. Enter your **old password**. The system then prompts you for a new password.

   c. Enter your **new password**, then re-enter the new password to verify your choice.

   d. Enter the **IP address** for the switch manager's Ethernet console.

   e. Enter the **subnet mask**.

   f. Enter the **default gateway** for the switch.

The following is a sample output of the **Setup** command to change or modify the Supervisor's Ethernet Console's IP address, subnet mask, default gateway or changing the super user password.

Welcome to Switch Setup. The brief series of questions that follows will help you to configure this switch. After completing this process, you will be able to manage the switch using:

- the switch-based HTTP server

- the Element Management System.

Text in [] is the default answer for each questions.

To accept the default, press ENTER.

Would you like to change the super user password [Yes]? Y

Old Password: xxxx

New Password: xxxx

Re-type New Password: xxxx

User password changed successfully

What do you want the switch manager's console

Ethernet IP Address to be [0.0.0.0]? 10.0.0.1

What is the subnet mask for your network's

IP address [0.0.0.0]? 255.255.255.0

What is the IP address of the default gateway for this network segment [0.0.0.0]?

You can now connect to the switch using the front-panel out-of-band 10Base-T connection. This allows you to log in using either the embedded Web Agent or the EMS.

See the Installation and Operation guides for instruction on establishing additional IP network connections.

## Connecting to the Supervisors 10/100Base-T port

Connect one end of a crossover patch cable to the 10/100Base-T on the Supervisor module front panel (Figure 2-1). Connect the other end to an out of band device.

Refer to Table 2-2 for an explanation of the pinouts for the 10Base-t crossover patch cable.

***Table 2-2. Pinouts for 10Base-T Crossover Patch Cables***

| Pin # | Color | Pin # | Color |
|---|---|---|---|
| 1 | WO | 3 | WG |
| 2 | O | 6 | G |
| 3 | WG | 1 | WO |
| 4 | B | 4 | B |
| 5 | WB | 5 | WB |
| 6 | G | 2 | O |
| 7 | WBr | 7 | WBr |
| 8 | Br | 8 | Br |

Open the Web Agent after you have completed the out-of-band connection. Refer to the "Opening the Web Agent" section later in this chapter.

# Configuring the Switch Using the Web Agent

The switch provides an embedded HTTP server that allows you to set all the switch's parameters from the Web Agent. You can use this interface for quick and simple configuration changes. Refer to Chapter 19, "Analyzing Network Performance By Using RMON and Ethernet Statistics" for information on monitoring and configuring the Avaya Multiservice switch.

Although this chapter provides detailed procedures explaining how to configure the switch using the Web Agent, the corresponding CLI commands to do the same task are listed after each procedure. Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Opening the Web Agent

Although the Web Agent supports any frames-capable browser, the system has been specifically qualified with the following browsers:

- Netscape Navigator 4.5 or later (but not version 6.0)
- Microsoft Internet Explorer 3.0 or later

*** Note:** If you use Microsoft Internet Explorer, version 5.30.2919.6307, and you click the **Back** button after you change a parameter on the Switch Port Configuration Web page, that parameter will change back to the previous setting and the switch will reset. If you change a number of parameters and click the **Back** button, the last parameter will change back to the original value and the switch will reset.

Use a later version of Microsoft Internet Explorer.

To open to the Web Agent:

1. Start your browser.
2. Enter the IP address for the switch you want to manage In the Location field. For example: http://10.91.7.23.

   If the TCP port for HTTP requests is set to a port number other than 80, you must specify the TCP port number in addition to the IP address to open the Web Agent. For example, if you change the TCP port from 80 to 9999 on switch 192.168.0.126, enter **http://192.168.0.126:9999** to

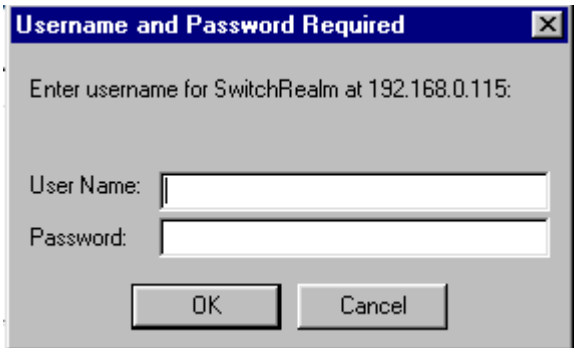
open the Web Agent. For information about how to change the TCP port for HTTP requests, see Changing the TCP Ports for HTTP and Telnet (page 43).

*** Note:** You must enter a separate IP address for each supervisor module interface (console or inband). For layer 3, you can use can any of the router interfaces.

3. Press Enter. The **Welcome to the Switch Management** window opens.

4. Select **Login**. The **Username and Password Required** window opens (Figure 2-2).

***Figure 2-2. Username and Password Required Window***



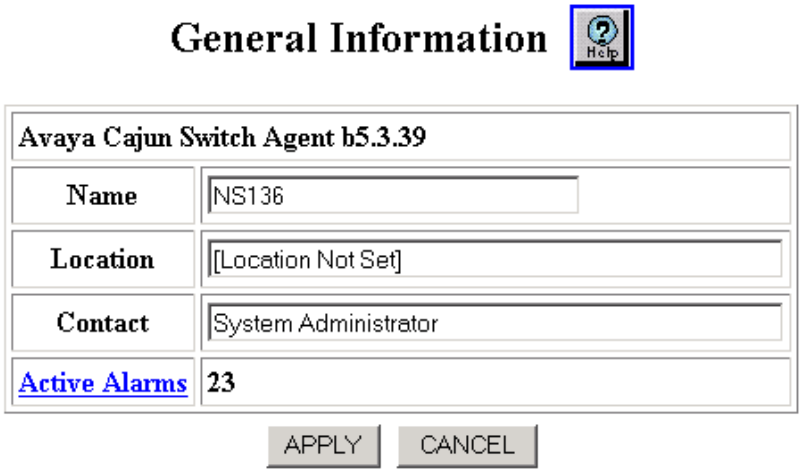

5. Enter a valid user name. The default super user name is **root.** Press the Tab key to move to the **Password** field.

6. Enter a valid password. The default password is **root**.

7. Select **OK**. The **General Information** window opens with the Web Agent group folders listed on the left (Figure 2-3).

*** Note:** To optimize security, change the root password for the system as soon as possible.

*Figure 2-3. General Information Window*

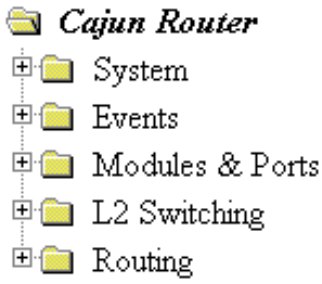



## Moving through the Web Agent

To move through the Web Agent screens:

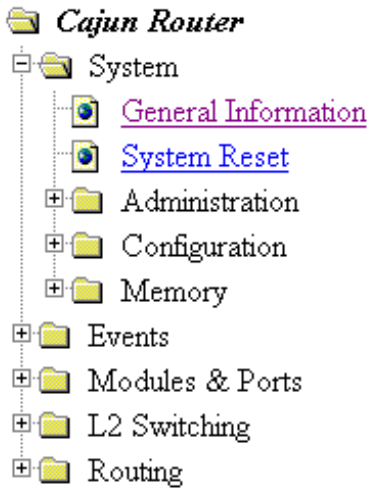
1. Select the plus sign (+) next to the folder that you want to open. That folder opens listing the operations you can perform (Figure 2-4).

*Figure 2-4. Opening a Web Agent Folder*




2. Select plus sign (+) next to the folder describing the operation you want to perform (i.e., Configuration). The folder opens listing the operations that you can perform (Figure 2-5).

*Figure 2-5. Operation Folder Contents*




3. Select an operation (i.e., **General Information**). The Web Agent dialog box for that operation opens on the right side.

4. Complete the operation.

*** Note:** The following configuration procedures are written assuming you have already logged onto the Avaya Multiservice Switch.

# Configuring Custom Access Types

This section provides the following information and procedures for configuring the Custom Access Types (CATs) on the Avaya P550R/ P580/P880/P882 Multiservice Switch:

- Opening the Custom Access Types Web Page
- Creating a Custom Access Type
- Modifying a Custom Access Type
- Deleting a Custom Access Type

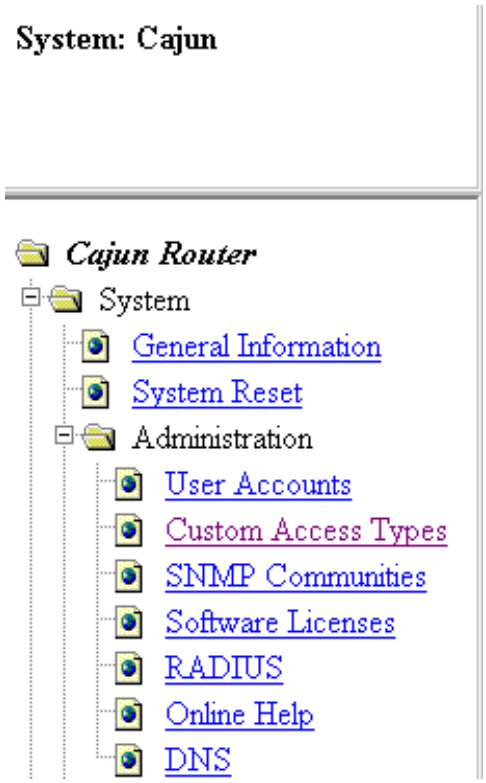
CATs allow a switch administrator to create a user profile with specific functional privileges. The functions are as follows: System Configuration, Modules & Port Management, Events Management, and L2 Routing and switching privileges. After creating one or more CATs (user profiles), the switch administrator can create a user account and assign a desired user profile to that account. After logging in, the user would be able to manage the switch based on the CAT applied to the account.

# Opening the Custom Access Types Web Page

To open the Custom Access Types Web page:

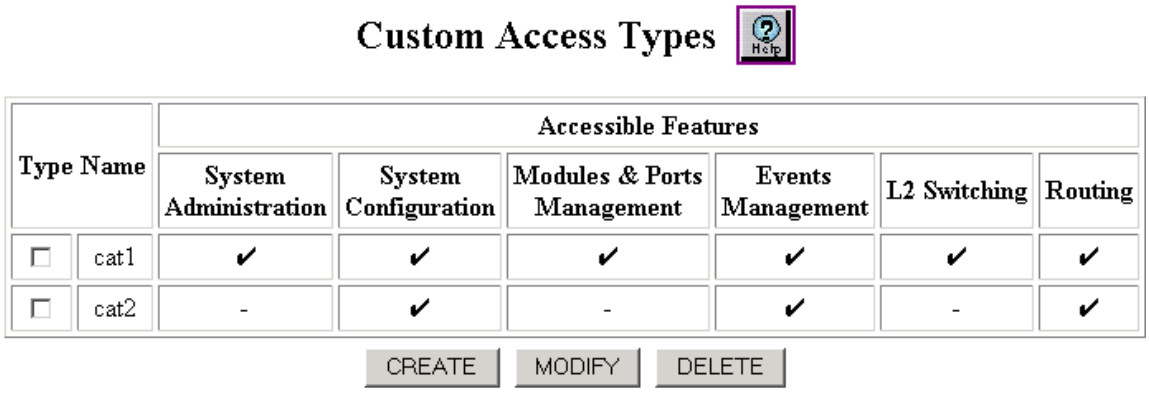
1. Select **System**>**Administration** from the left side of the switch web screen (Figure 2-6)

***Figure 2-6. Opening the Custom Access Types Web Screen***




2. Select **Custom Access Types. The Custom Access Types** web screen displays (Figure 2-7).

*Figure 2-7. Custom Access Types Web Screen*




## Creating a Custom Access Type

To create a Custom Access Type:

1. Open the **Custom Access Types** web screen (refer to the "Opening the Custom Access Types Web Page" section earlier in this chapter).
2. Select **Create** from the **Custom Access Types** web screen. The **Create Custom Access Type** screen displays (Figure 2-8).

*Figure 2-8. Create Custom Access Type Screen*

3. Type a name in the **Type Name** field. You can type up to 32 characters.

4. Select which features that you want this access type to support from the **Accessible Features** list.

5. Select **Apply** to save the Access Type or **Cancel** to ignore the Access Type.

### Creating Custom Access Types with the CLI

To create a Custom Access Type using the CLI, enter the following command in Configuration mode:

```
<configure># custom-access-type <catName> [sys-
configuration] [module-port-mgmt] [events-mgmt
] [l2-switching] [routing]
```

## Modifying a Custom Access Type

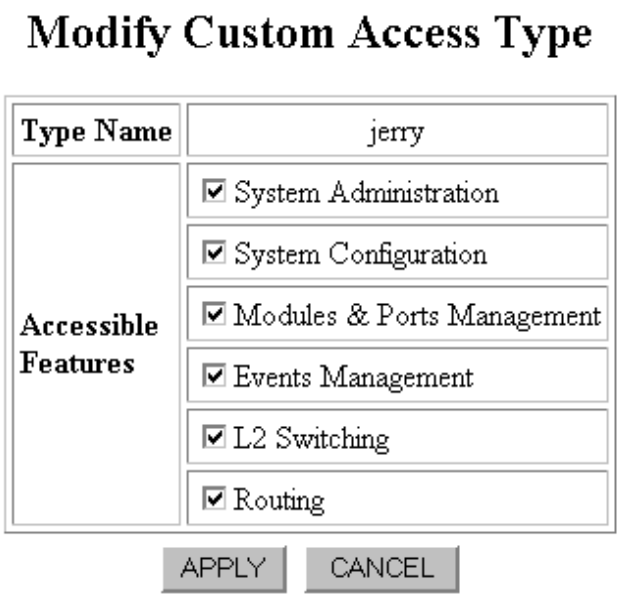
To modify a Custom Access Type:

1. Open the **Custom Access Types** web screen (refer to the "Opening the Custom Access Types Web Page" section earlier in this section).

2. Select an access type name from the **Type Name** field.

3. Select **Modify** from the **Custom Access Types web screen.** The **Modify Custom Access Type** web screen displays with the name of the access type you want to modify displayed in the **Type Name** field (Figure 2-9).

*Figure 2-9. Modify Custom Access Type Web Screen*




4. Select or de-select the accessible features you want to add or remove for this access type from the **Accessible Features** list.

5. Select **Apply** to save the modification to the specific access type or **Cancel** to ignore the modifications.

*** Note:** You can not modify an existing Custom Access Type with a CLI command.

## Deleting a Custom Access Type

To delete a custom access type:

1. Open the Custom Access Types web screen (refer to the "Opening the Custom Access Types Web Page" section earlier in this chapter).

2. Select an access type from the **Type Name** field.

3. Select **Delete** from the **Custom Access Types** web screen. The **Delete Custom Access Type** confirmation screen displays with the access type name listed in the **Custom Access Type** field (Figure 2-10).

*Figure 2-10. Delete Custom Access Type Confirmation Screen*

Delete Custom Access Type
Help
WARNING: User accounts that have been created with these access types will be affected
Users with these access types will no longer be able to log into the switch.
Delete following Custom Access Types?
Custom Access Type:
Private
YES
NO

4. Select **Yes** to delete the selected Access Type or **No** to keep the access type.

   *** Note:** User accounts that have been created with this access type will no longer be able to log into the switch.

### Deleting a Custom Access Type using the CLI

To delete a Custom Access Type using the CLI, enter the following command in Configuration mode:

```
<configure># no custom-access-type <cat name>
```

## Setting Up User Accounts

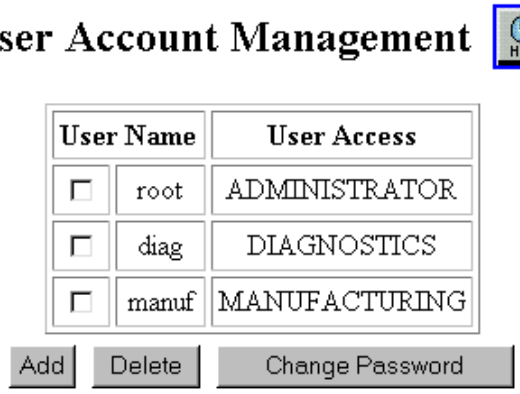
You can setup **User Accounts** using either the Web Agent or the CLI.

### Setting Up User Accounts Using the Web Agent

To setup a user account using the Web Agent:

1. Select **User Logins** from the **System > Administration** group on the Web Agent window. The **User Account Management** dialog box opens (Figure 2-11).

*Figure 2-11. User Account Management Dialog Box*




2. Select **Add**. The **Add User Account** dialog box opens (Figure 2-12).

*Figure 2-12. Add User Account Dialog Box.*

3. Enter a user name in the **User Name** field. (up to32 characters)

4. Enter a password in the **Password** field. (up to 32 characters)

   *** Note:** Do not use the combination of these special characters for the user login password (#, $,%, ^, &, *, (,).

5. Re-type the password in the **Re-enterPassword** field.

6. Select an access type from the **Access Type** field pull-down menu. The options are:

   - READ_ONLY
   - READ_WRITE
   - ADMINISTRATOR
   - Custom Access Types - The Custom Access list names you created will display (previously configured Custom Access Type see the section "*Creating a Custom Access Types*" for more information)

7. Click in the checkbox to select the **Management Type** for the user.

   - Local CLI, from the Supervisor's serial console
   - Remote CLI, through a Telnet Session
   - Web, management from the Web agent

8. Select **Apply** to create the user account and a access type or select **Cancel** to ignore.

### Setting Up User Accounts Using the CLI

To setup a user account using the CLI, enter the following command in Configuration mode:

```
<configure>#username <name> password [encrypted-
type1] <passwd> [access-type {read-only|read
-write|admin|<catName>}] [mgmt-type [all][local-
cli][remote-cli][web]]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Disabling User Accounts

### Web Agent Procedure

For security reasons, you may want to disable certain user accounts, such as the **manuf** and **diag** accounts.

To disable user accounts by using the Web Agent:

1. Expand the **System** > **Administration** folders.
2. Select **User Accounts**.

   The User Account Management Web page opens.

3. Select the check box next to the **manuf** or **diag** account that you want to disable.
4. Select **Modify**.

   The Modify User Account Web page opens.
5. In the **Status** field, select **Disable**.

### CLI Command

To disable the user accounts using the CLI, enter the following CLI command:

**Avaya>username {names} access-type {enable | disable}**

Where name is the user account name.

## Setting Up SNMP Communities

SNMP is identified on a switch through SNMP communities. SNMP communities are configured to manage the switch. You set up SNMP communities using either the Web Agent or the CLI.

*** Note:** SNMP Version 2c is supported.

All three switches support a maximum of ten SNMP community strings.

### Setting Up SNMP Communities Using the Web Agent

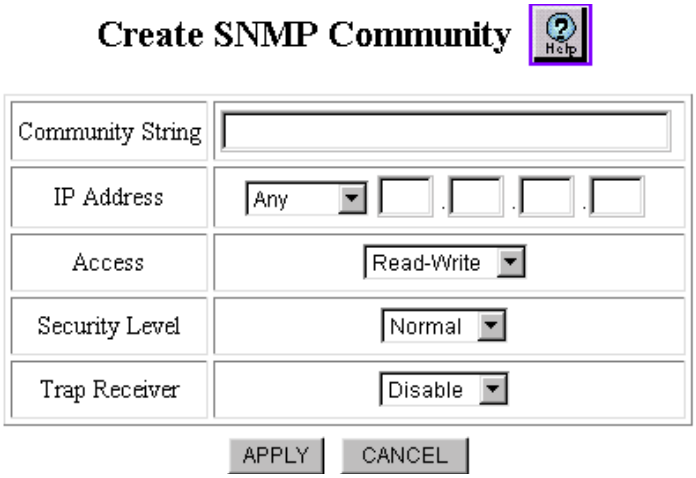
To set the SNMP communities parameters using the Web Agent:

1. Select SNMP Administration from the **System > Administration** folder on the Web Agent. The **SNMP Community Management** window opens (Figure 2-13).

***Figure 2-13. SNMP Community Management Window***

2. Select **CREATE**. The **Create SNMP Community** dialog box opens (Figure 2-14).

*Figure 2-14. Create SNMP Community Dialog Box*




3. Enter a name for the SNMP community in the **Community String** field.

4. Select an option from the **IP Address** field pull-down menu. The options are:

   - Any – for any IP address
   - Specific – Enter an IP Address.

   *** Note:** You cannot enable the trap receiver if you select Any.

5. Select an access level for this community from the **Access** field pull-down menu. Refer to Table 2-3 for the Access level field options.

*Table 2-3. Access Level Field Options*

| Access Level | Manager Can... | Manager Cannot... |
|---|---|---|
| **Read-Only** | View switch configuration settings and statistics. | View community strings. Change switch configurations. |
| **Read-Write** | View and set switch configuration settings, and view statistics. | View community strings. |
| | | ***1 of 2*** |

*Table 2-3. Access Level Field Options continued*

| Access Level | Manager Can... | Manager Cannot... |
|---|---|---|
| **Read-Write with Security Level Set to admin** | View and set all switch parameters, including community table. | N/A |
| **None** | Disable a string without deleting it. | Access any switch features. |
| | | *2 of 2* |

6. Select a security level from the **Security Level** pull-down menu (refer to Table 2-4).

*Table 2-4. Security Level Field Options*

| Option | Allows Access to... |
|---|---|
| **normal** | All switch configuration and reporting functions. |
| **admin** | All switch configuration and reporting functions, including access to **community configuration**. |
| **Custom Access Types (if defined)** | All switch configuration and reporting functions, including access to **community configuration**. |

7. Select **Enable** from the **Trap Receiver** field pull-down menu. The default is **Disable.**

   *** Note:** Select **Enable** only if you selected **Specific** from the **IP Address** field.

8. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

   *** Note:** If you click **Apply**, the changes are saved in the Running config only. The Startup Config has not changed. Therefore, these and other changes will be lost if your switch goes down or if you power it off.

   To save these changes, you must copy the Running config as the Startup configuration. Refer to the section “Copying Configuration Files" section later in this chapter.

### Setting Up SNMP Communities Using the CLI

To set the SNMP communities parameters using the CLI, enter the following command:

```
<configure># snmp-server community
<community-string>{none|ro|rw}[{normal|
admin}] <catName|ip-addr|admin|normal>
<CR|IP-Addr>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

*** Note:** To disable SNMP, you must set the access for all community strings to **None**. You cannot disable SNMP by deleting all community strings because the public community string is restored when you reboot the switch.

9. Select or de-select the accessible features you want or want to remove for this access type from the **Accessible Features** list.

10. Select **Apply** to save the modification to the specific access type or **Cancel** to ignore the modifications.

# Configuring User Accounts

You can add a custom access type to a user through the User Accounts field.

To add a custom access type to a user:

1. Select **System**>**Administration** from the left side of the switch web screen.

2. Select **User Accounts**. The **User Accounts** web screen displays.

3. Select **Add**. The **Add User Account** web screen displays.

4. Type a user name in the **User Name** field. The user name may contain up to 32 characters.

5. Type a password in the **Password** field and re-type the password in the **Re-enter Password** field. The password may contain up to 32 characters.

6. Select the scroll arrow located on the right of the Access List field. The custom access list names you created will display.

7. Select a custom access list name for the user.

8. Select Apply to give the user the access type or select Cancel to ignore.

# Remote Authentication Dial-In User Service (RADIUS) Client Support

## Overview of RADIUS

In a network with many Avaya switches, it can become difficult to keep track of all of the user accounts on each of the switches. You can centralize the user accounts by using a RADIUS server.

RADIUS is a service that authenticates users when they attempt to log into a Network Access Device (NAD) such as an Avaya switch. RADIUS typically runs on a Windows or Linux server however, it can run on other platforms as well depending upon the vendor.

RADIUS is a client/server architecture where each device that uses the RADIUS server is a RADIUS client. The client sends an Access Request messages to the RADIUS server. These messages include the user's login name, the password encrypted, and optional parameters depending on configuration.

*** Note:** It is critical that the RADIUS Client and Server be configured with the exact same parameters.

Once received, the RADIUS server will look through its database for the user account. If it finds an account, the password is correct, and the optional parameters match, an Access Accepted message is returned to the RADIUS client indicating that the user account exists, the password was correct, and the user has a certain access type (for example: Administrative or Read-Only). If not found, the password is incorrect, or the optional parameters don't match, then an Access Rejected message is sent.

## Standard RADIUS

A standard RADIUS configuration provides two types of access (a.k.a. Service-Types): Administrative or Read-Only. This happens when a Group name is ***not*** specified and no additional parameters are configured on the RADIUS server for the user account. In the case of the Avaya switch, this implies that a user is given Administrative or Read-Only access. The Avaya switch includes a third type of access, Read-Write, which cannot create other user accounts but can configure the switch. If you are using a Standard

RADIUS configuration, you will not be able to create user accounts that are Read-Write.

## Realms & Groups

Realms and Groups provide two separate functions. A Realm provides a way of organizing user accounts on the RADIUS server. Groups provide a way of organizing NADs a user can log into as well as delivering vendor specific configurable parameters.

For example: You might use a Realm called AvayaRealm to organize all of the user accounts that can log into Avaya switches in a campus environment. In this campus, there are two teams of network administrators, one team for the North campus and one for the South campus. Each team needs Read-Write access to the switches in their half of the campus and Read-Only access to the switches in the other half of the campus.

You would then configure all of the North switches with a Group name of NorthSwitches; and the South switches with SouthSwitches.

For each user, you would create two user accounts in the AvayaRealm, one with a Group name of NorthSwitches and one with SouthSwitches. Each account would have the appropriate permissions for the two switch types.

When a user from the North team logs into a switch in the North campus, the switch will send an Access Request message with @AvayaRealm appended to the user name and a Group name of NorthSwitches. The RADIUS server will send an Access Accept message indicating Read-Write permission.

Similarly, when the same user logs in to a switch on the South campus, the message will append @AvayaRealm and a Group name of SouthSwitches. The RADIUS server will send an Access Accept message indicating Read-Only permission.

## Realms

A Realm provides a mechanism by which a RADIUS manager can organize user accounts. Consult the RADIUS vendor's documentation on how to create Realms on the server. Once created, user accounts are placed in the realms. The realm name is also configured on the NADs and when the NADs send Access Request messages, the user name is appended with an "@" and the Realm name.

For example: User Bob in the AvayaRealm would log into the switch with Bob. The Avaya switch would send the Access Request

message with user Bob@AvayaRealm. The RADIUS server, upon receiving the request, would look for Bob in the AvayaRealm.

## Groups & RADIUS with Vendor Specific Attributes (VSA)

In order to provide user accounts with the same granularity of privileges as on the Avaya switch, Vendor Specific Attributes must be configured on the RADIUS server and a Group name ***must*** be set on the Avaya switch. When set, the Group name is sent along with the Access Request message to the RADIUS server.

The RADIUS server will send an Access Accept message if the user name, password, and Group name match that of the user account. If so, the Access Accept message will include the VSAs that identify the privileges the user has.

*** Note:** If a user has a Standard RADIUS account, one that does not contain the Group name, the RADIUS server will still respond with an Access Accept message; but the message will not contain the Group name or the VSAs. This is a security loophole. See the **Avaya-Service-Type-Required** parameter below for more information

Avaya Service-Types specify the level of privileges a user has. The following three types are supported:

- Administrative (can create user accounts and configure the Avaya switch)
- Read-Write (can configure the Avaya switch)
- Read-Only (can view the Avaya switch configuration)

Avaya Management Types specify what method the user can use to manage the switch. The following four types are supported:

- Avaya Management All
- Avaya Local CLI (Serial port on the supervisor)
- Avaya Remote CLI (Telnet session)
- Avaya Web Agent

## Custom Access Types(CAT)

Custom Access Types provide a deeper level of granularity with regards to what parameters a user can configure. For example, you could restrict a user to configuring Layer 2 parameters only. If you need to use CATs, those user accounts must be created and stored locally on the Avaya switch, not on a RADIUS server.

## Login Order of Operations

When a user attempts to log into the Avaya switch, the switch will first check the local user accounts for the entered user name and password. If found, the user is logged in using the local settings for that account.

If no local account is found and RADIUS is enabled/configured, the switch will send an Access Request message to the primary RADIUS server in an attempt to authenticate the user remotely. If the user's login is found and correct, then the RADIUS server responds with an Access Accept message that includes the user's privileges. Provided the user account has the right Management Type (for example: Web Agent if you are trying to log in to the embedded Web Agent), the user is granted access.

If the user's login is incorrect or does not exist, then a Access Reject message is sent to the switch and the user is denied access to the switch.

If the RADIUS server does not respond, the Avaya switch will attempt to use the Secondary server if it is configured, and if not, will continue to try the Primary. If the Secondary server is configured, the switch will alternate between the two servers on subsequent retries. It will wait the number of seconds specified in the retry interval and try as many times as specified in the retry time.

## RADIUS Client File settings

Consult the RADIUS server's documentation for information on configuring Client and User files. The following tables list the Avaya attributes and values for each of the Avaya attributes.

***Table 2-5. Avaya Specific Attributes***

| Attribute Name | Attribute Values | Attribute Specific Description | Attribute Specific Value |
|---|---|---|---|
| Avaya-Service-Type | 1 | Avaya-Read-Only | 1 |
| | | Avaya-Read-Write | 2 |
| | | Avaya-Administrative | 3 |
| Avaya-Management-Type | 2 | Avaya-Mgt-All | 1 |
| | | Avaya-Local-CLI | 2 |
| | | Avaya-Remote-CLI | 3 |
| | | Avaya-Web | 4 |
| Avaya-Group | 3 | <group name> | |

## Sample User File

The following is a sample user file. Each RADIUS vendor may have a different method for configuring User files. In this sample, text values are defined that represent the actual values used by the Avaya switch using the directives ATTRIBUTE and VALUE.

Two user accounts are shown a Standard RADIUS account and an account with VSAs. The first account is “Bob” with password “BooBoo”. Bob is only allowed to log in to the NAD at 199.87.201.2. Bob is also granted Administrative privileges.

The second account is “Ann” with password “Pokey”. The NAD she logs in to must be configured to use group “AvayaSwitches”. She is granted Read-Only permission using the CLI (either Telnet or serial cable to the supervisor’s console port).

```
# define the Avaya Vendor Specific Attributes
ATTRIBUTE Avaya-Service-Type
ATTRIBUTE Avaya-Mgt-Type
ATTRIBUTE Avaya-Realm
ATTRIBUTE Avaya-Group
# Note: NAS-IP-Address is a Standard RADIUS Attribute

# define the Avaya-Service-Types
VALUE Avaya-Service-Type Avaya-Administrative 3
VALUE Avaya-Service-Type Avaya-Read-Write 2
VALUE Avaya-Service-Type Avaya-Read-Only 1

# define the Avaya Management Types
VALUE Avaya-Mgt-Type Avaya-Mgt-All 1
VALUE Avaya-Mgt-Type Avaya-Console-CLI 2
VALUE Avaya-Mgt-Type Avaya-Remote-CLI 3
VALUE Avaya-Mgt-Type Avaya-Web 4

# define User Accounts
Bob   Password = "BooBoo", NAS-IP-Address = "199.87.201.2"
      Service-Type = Administrative
Ann   Password = "Pokey", Avaya-Group = "AvayaSwitches"
      Avaya-Service-Type = Avaya-Read-Only
      Avaya-Management-Type = Avaya-Local-CLI
      Avaya-Management-Type = Avaya-Remote-CLI
```

## Sample Client File

The following is a sample Client file. Client files hold the IP address(es) of the NADs and their associated Shared Secrets. Client files may vary from vendor to vendor. Consult the vendor documentation on how to configure Client files.

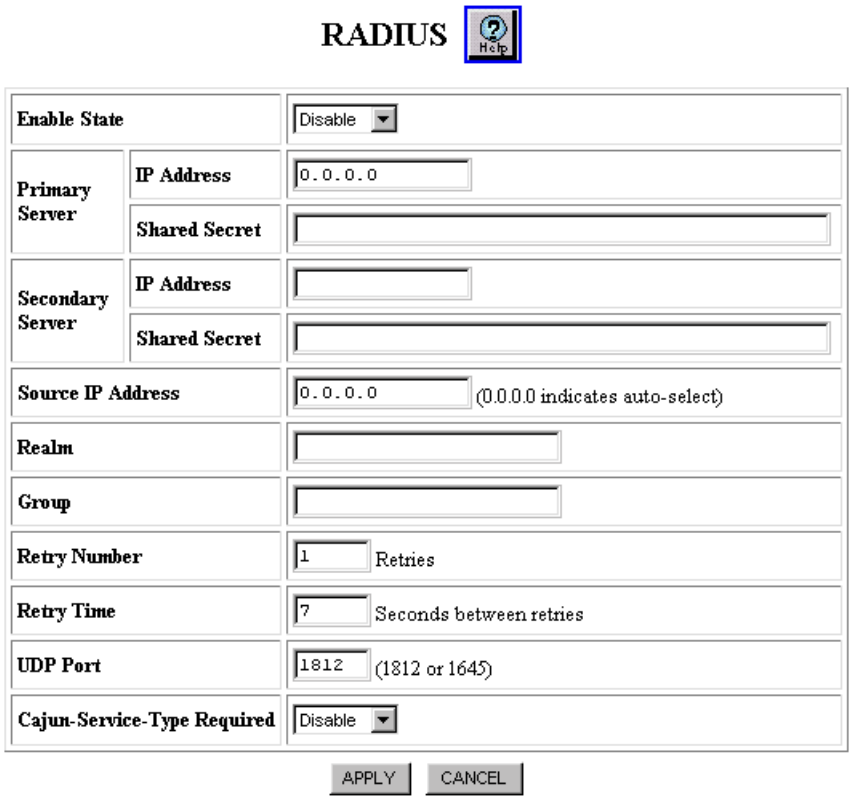
```
#Client Name                    Shared Secret
#----------------------------   ----------------------
199.87.201.2                    W3ftrFF4
10.30.44.1                      Gruuf66
```

## Configuring a RADIUS Client Using the Web Agent

To configure a RADIUS client using the Web Agent:

1. Select **RADIUS** from the **System > Administration** group on the Web Agent window,. The **RADIUS** dialog box opens (Figure 2-15).

***Figure 2-15. RADIUS Dialog Box.***




2. Select **Enable** from the **Enable State** field pull-down menu.

3. Refer to Table 2-6 to configure the RADIUS dialog box configuration parameters;

***Table 2-6. RADIUS Dialog Box Configuration Parameters***

| Parameter | Definition |
|---|---|
| **Enable State** | Enable or disable RADIUS on the switch. |
| **Primary Server** | • **IP Address** - Enter the IP address for the Primary RADIUS server.<br>• **Shared Secret** - Enter the Shared Secret the switch will use for encrypting/decrypting passwords. Make sure the Primary server is configured with the exact same characters (case sensitive). This value is itself encrypted and will not be displayed anywhere (Web Agent or CLI) once set. It can be changed by simply entering in a new shared secret. |
| **Secondary Server** | • **IP Address** - Enter IP address for the Secondary RADIUS server.<br>• **Shared Secret** - Enter the Shared Secret the switch will use for encrypting/decrypting passwords. Make sure the Secondary server is configured with the exact same characters (case sensitive). This value is itself encrypted and will not be displayed anywhere (Web Agent or CLI) once set. It can be changed by simply entering in a new shared secret. |
| **Source IP Address** | Enter an IP interface address the switch will use as the source IP address in the Access Request messages. This value must be an IP interface address on the switch. If set, and the IP interface becomes disabled, RADIUS will not function because the switch will not be able to send or receive RADIUS messages.<br>If left 0.0.0.0 (the default), the switch will automatically select (auto-select) a source IP address from one of its active interfaces. This implies you will have to add each of the switch's IP addresses to the Client file on the RADIUS server since you won't be guarantying the source IP address. |
| **Realm** | Only set this parameter if Realms are used on the RADIUS server for organizing user accounts. If so, enter the ASCII text Realm name for the user accounts authorized to log into the Avaya switch.<br>This implies that any user account authorized to log into this switch must reside in the same Realm. |
| | ***1 of 2*** |

*Table 2-6. RADIUS Dialog Box Configuration Parameters*

| Parameter | Definition |
|---|---|
| **Group** | Enter the ASCII Group name.The Group name will be included in the Access Request message sent to the RADIUS server.<br>This implies that user accounts are configured with a Group name on the RADIUS server and that the Vendor Specific Attributes are set for the user accounts.<br>(See also Avaya-Service-Type-Required below) |
| **Retry Number** | Enter the number of times to re-send the Access Request message if there is no response. |
| **Retry Time** | Enter the time (in seconds) to wait before re-sending an Access Request message. |
| **UDP Port** | Enter the UDP port number. The default value is **1812**. Valid options are 1812 or 1645 only. |
| **Avaya-Service-Type Required** | If enabled, the switch will only honor Access Accept messages that have the correct Group name included. This setting prevents the switch from incorrectly allowing access to users that may have a user account on the RADIUS server but should not be allowed access to the switch.<br>This could occur if user "Bob" has a Standard RADIUS user account with Administrator (or Read-Only) privileges. When Bob logs in, the RADIUS server will authenticate him and respond with an Access Accept message of Administrator but will not include the VSAs and Group name associated with the Avaya switch. This implies anyone who has a Standard Account will be able to log into the Avaya switch.<br>By enabling this setting and explicitly configuring user accounts with the Avaya specific attributes and Group name, you will have tighter control over the security of the Avaya switch. |
| | ***2 of 2*** |

## Configuring a RADIUS Client Using the CLI

To configure a RADIUS client using the CLI, enter the following command from **Enable/Configure** mode:

```
<configure># set radius authentication
<parameters>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for more details about this command.

# Changing the Console Serial Port Settings

You can change the communications settings for the serial port connection located on the front panel of the layer 3 supervisor module from the Web Agent. The switch's console port is initially configured as a TTY Console to support a TTY connection. The layer 2 and layer 3 supervisor modules allow you to reconfigure the console serial port as a PPP Console to support a dial-in PPP connection using a modem.

*** Note:** If you reconfigure the serial port as a PPP console, you can only change the switch's baud rate and flow control parameters. The flow control parameters are limited to None or Xon/Xoff.

## Configuring the Serial Console Port as a TTY Console

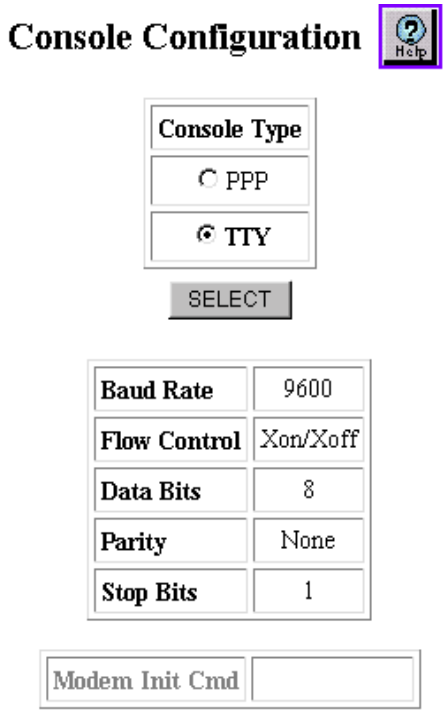
You can configure the serial port as a TTY console using either the Web Agent or the CLI.

### Configuring the Serial Console Port as a TTY Console Using the Web Agent

To configure the console serial port as a TTY Console using the Web Agent:

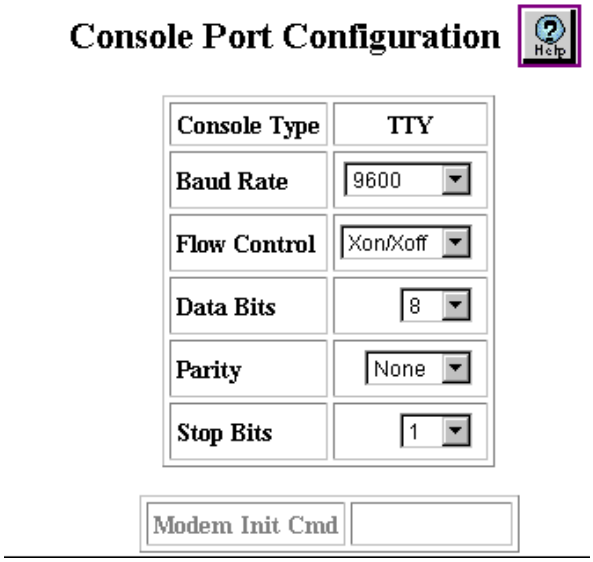
1. Select **Console Configuration** from the **System> Configuration** group on the Web Agent. The **Console Configuration** window opens (Figure 2-16).

*Figure 2-16. Console Configuration Window*




2. Select **TTY** as the console type and click **SELECT**. The **Console Port Configuration** window opens with TTY displayed in the **Console Type** field (Figure 2-17).

*Figure 2-17. Console Port Configuration Window.*




3. Refer to Table 2-7 and configure the other **Console Port Configuration** dialog box parameters:

*Table 2-7. Console Port Configuration Dialog Box Parameters*

| Option | Default | Available Settings |
|---|---|---|
| **Baud Rate** | 9600 | 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 |
| **Flow Control** | Xon/Xoff (TTY) | None, Xon/Xoff (TTY) |
| **Data Bits** | 8 | 7 or 8 |
| **Parity** | None | Odd, Even, or None |
| **Stop Bits** | 1 | 1 or 2 |

4. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

## Configuring the Serial Console Port as a TTY Console Using the CLI

To configure the console serial port as a TTY Console using the CLI, enter the following command:

```
>set console type {tty|ppp}
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Configuring the Serial Console Port as a PPP Console

You can reconfigure the serial port as a PPP console to support a dial-in PPP connection using either the Web Agent or the CLI. Before you can do so, however, you must connect a modem to the switch.

*** Note:** If you do not configure an IP address for the PPP serial interface, the switch immediately sends the modem configuration string. If you type TTY, you will re-access the CLI login prompt.

## Connecting a Modem

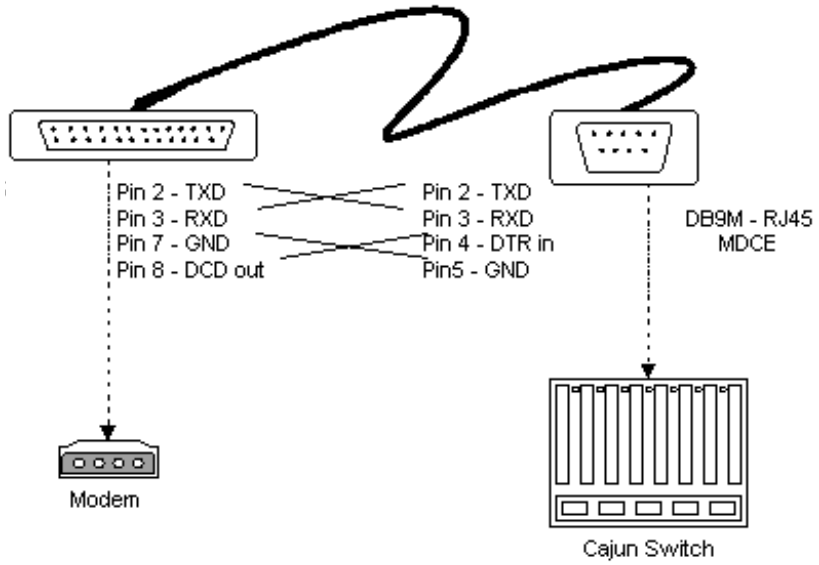
After you connect a modem to your switch with the specified serial cable and connectors, and configure the serial port in PPP mode, the switch will convert the normal Distributed Computing Environment (DCE) interface to a Data Terminal Equipment (DTE) interface that is used by modems.

It then periodically sends the modem configuration string from the serial console port. This synchronizes the baud rates between the modem and the console port and configures the modem to operate with the switch's DTE interface.

To connect a modem (Figure 2-18):

1. Attach a DB25M-RJ45 (P/N 38210003) connector to the modem.
2. Attach the DB9M-RJ45 MDCE connector to the switch's serial console port on the front panel of the switch.

*Figure 2-18. Typical Modem Connection to a Switch*

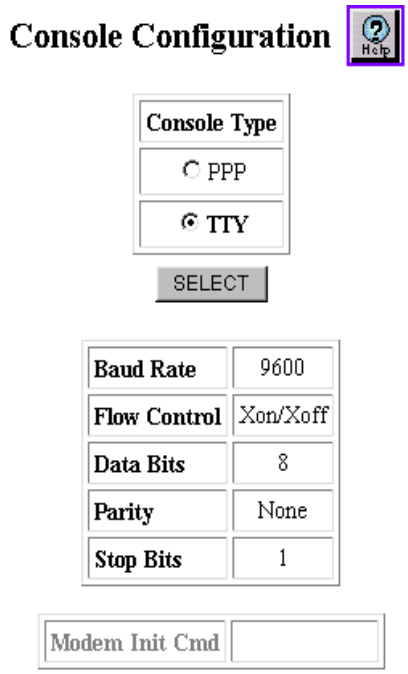



## Using the Web Agent

To configure the console serial port as a PPP console from the Web Agent:

1. Select **Console** from the **System > Configuration** group on the Web Agent. The **Console Configuration** dialog box opens (Figure 2-19).

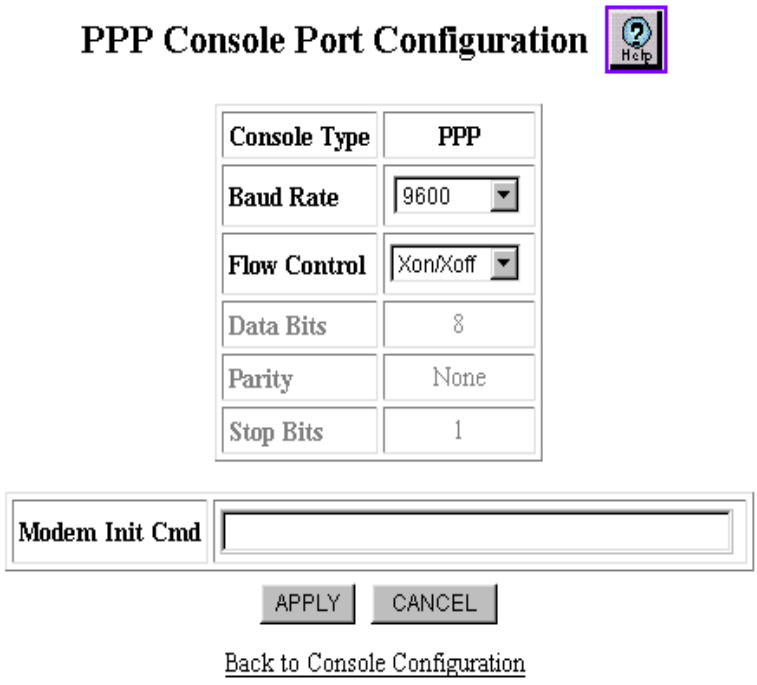
*Figure 2-19. Console Configuration Window*




2. Select **PPP** as the console type and click **SELECT**. The **Console Port Configuration** window opens with **PPP** displayed as the Console Type (Figure 2-20).

*** Note:** If you select **PPP**, the **PPP Console Port Configuration** dialog box opens.

*Figure 2-20. PPP Console Configuration Window.*




3. Select a baud rate from the **Baud Rate** field pull-down menu that is different from the one already selected.

4. Select an option from the **Flow Control** field pull-down menu. The options are: None and Xon/Xoff.

   *** Note:** You can only change the baud rate and flow control parameters after you configure the serial port as a PPP console.

5. Enter the modem initialization command in the **Modem Init Cmd** field. The default modem configuration init command is AT&D0SO=1.

   Refer to Table 2-8 for a definition of the Modem Configuration Init command parameters.

*Table 2-8. Modem Configuration String Parameters*

| Parameter | Definition |
|---|---|
| **&D0** | Disable DTR |
| **S0=1** | Auto-answer mode (one ring) |
| **CD follows carrier** | Depends on modem |
| | ***1 of 2*** |

*Table 2-8. Modem Configuration String Parameters*

| Parameter | Definition |
|---|---|
| **E0** | Disable local echo |
| **Software Flow Control (Receive and Transmit)** | Depends on modem |
| | *2 of 2* |

*** Note:** If you misconfigure the PPP serial console port, you can regain CLI access to correct the configuration parameters. For more information, refer to the "Using the CLI" section later in this chapter.

**Safety Tip:** To successfully dial-in with PPP to the switch, you must also configure an IP address and interface for the PPP Serial Interface (Serial-Console). Refer to "Managing Configuration Files", later in this chapter for more information.

6. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

*** Note:** If you click **Apply**, the changes are saved in the Running config only. The Startup config has not changed. Therefore, these and other changes will be lost if your switch goes down or if you power it off. To save these changes, you must copy the Running config to the Startup config. Refer to the Copying Configuration Files section later in this section.

## Using the CLI

To configure the console serial port as a TTY Console using the CLI after you install a mode, enter the following command in Configure mode:

```
>(configure)# set console type {tty|ppp}
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

### Regaining Configuration Access to the PPP Serial Port Console

If you incorrectly configure the PPP serial port console, you cannot regain configuration access to the Web Agent or the CLI. This is a temporary situation and can corrected.

To regain configuration access to the Web Agent or the CLI when the console port is in PPP mode:

1. Enter `TTY` in the console window. The CLI login prompt displays. It may be necessary to press Enter several times to see the login prompt. You may see the modem init command string.
2. Enter your user name at the **Login** prompt. The password prompt displays.
3. Enter your password at the **Password** prompt. The switch CLI prompt displays.

   Enter the PPP configuration commands necessary to start PPP. Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about these PPP commands.
4. Enter **`exit`** at the CLI prompt after you complete your configuration settings to reinvoke the modem control software and exit CLI mode.

*** Note:** You do not need to exit from CLI if the serial port console has been configured as a TTY console, or if you do not intend to re-attempt connecting using PPP.

# Configuring Dial-Up Networking

To configure your PC for dial-up networking with a PPP serial port console:

1. Open **My Computer** on your PC.
2. Double-click **Dial-Up Networking**. The **Dial-Up Networking** window opens.

   *** Note:** You must have dial-up networking installed on your PC.
3. Double-click **Make New Connection** to configure your modem. The **Make New Connection** wizard opens.

4. Enter a connection name for the computer you are dialing in the Type a name for the computer you are dialing field.
5. Open the **Select a Modem** pull-down menu.
6. Select your modem and select **Configure**. The **Modem Properties** window opens.
7. Select the **Connection** tab. The **Connection** window opens.
8. Select the following from the **Connection Preferences** window:
   - Open the Data bits pull-down menu and select 8.
   - Open the Parity pull-down menu and select None.
   - Open the Stop bits pull-down menu and select 1.
9. Select **Advanced**. The **Advanced Connection Settings** window opens.
10. Select Software (XON/XOFF) from the **Use flow** control field.
11. Select **OK** to close the window. The **Modem Properties** window re-opens.
12. Select the **Options** tab. The **Options** window opens.
13. Select **Bring up terminal window** after dialing from the **Connection Control** field. Select **OK**. The **Modem Properties** window closes and the wizard continues.
14. Select **Next** from the wizard window and enter the telephone number you are calling.
15. Select **Next**. The wizard reports that you have successfully configured a modem.
16. Select **Finish**. The wizard closes and the newly configured connection displays in your Dial-Up networking program group.
17. Select your new connection right click the mouse.
18. Select **Properties**. The **Properties** window opens.
19. Select the **Server Types** tab and de-select all advanced options except TCP/IP.
20. Select **TCP/IP** Settings. The **TCP/IP Settings** window opens.

21. Select Specify an IP Address and enter the IP address fro the serial port interface.

22. Select **Server** assigned name server addresses.

23. De-select **Use IP header Compression** and **Use Default Gateway** on remote network.

24. Select **OK** to close the TCP/IP window.

25. Select **OK** to close the **New Connections Properties** window.

## Using Dial-Up Networking with a PPP Serial Port Console

To use TCP/IP applications (Telnet, HTTP, and SNMP) over your PPP serial port interface:

1. Open **My Computer** on your PC.

2. Double-click **Dial-Up Networking**. The **Dial-Up Networking** program group opens.

   *** Note:** You must have dial-up networking installed on your PC.

3. Double-click the PPP modem you previously created. The **Connect To window** opens.

4. Enter your password and select **Connect**. A **Pre-Dial Terminal** Screen opens.

   When the modem has successfully connected, a **Post-Dial Terminal** Screen opens.

5. Login in the **Post-Dial Terminal** screen using your CLI user name and password. It may be necessary to enter several carriage returns to view the Login prompt.

6. At the CLI prompt, go to configuration mode.

7. Enter **`set console transfer PPP`**. ASCII characters display below the CLI prompt. This is typical while the switch attempts to connect via PPP.

8. Select **Continue** (F7) from the **Post-Dial Terminal** screen. PPP verification completes and the **Connected To** window displays a message that the modem connection has been successfully established.

# Changing the TCP Ports for HTTP and Telnet

## Overview

For security purposes, you may want to change the TCP port number for Telnet requests and HTTP requests. The default settings for these ports are the well-known TCP ports. HTTP requests use TCP port 80, and Telnet requests use TCP port 23.

Once you change the TCP port number for HTTP, only users who know the new port number can open the Web Agent. And once you change the TCP port for Telnet, only users who know the new port number can start Telnet sessions to the switch.

When you change the TCP port number for either of these protocols, the change takes effect immediately and all connections through the previous port number are disconnected. Any changes that you make to these TCP port numbers are retained if you reset the switch or if the primary supervisor module fails over to the standby supervisor.

This section contains procedures for the following tasks:

- Changing the TCP Port Number for HTTP and Telnet Requests (page 43)
- Starting a Telnet Session (page 45)
- Opening the Web Agent (page 46)

You must have administrative privilege to view or change the TCP port for HTTP or Telnet.

## Changing the TCP Port Number for HTTP and Telnet Requests

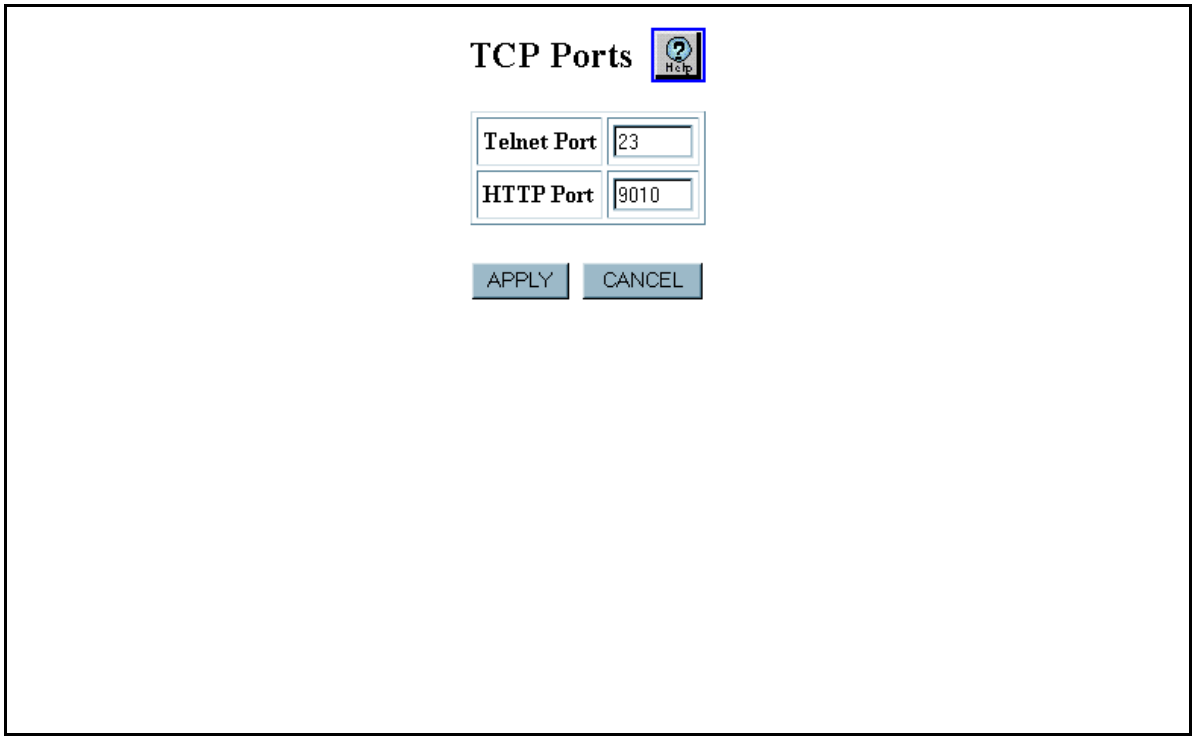
### Web Agent Procedure

To change the TCP port for HTTP requests or Telnet requests by using the Web Agent:

1. In the navigation pane, expand the **System** > **Administration** folders.
2. Click **TCP ports**.

   The TCP Ports Web page is displayed in the content pane. See Figure 2-21.

*Figure 2-21. TCP Ports Web page*




3. To change the TCP port for Telnet requests, in the **Telnet Port** field, enter the port number that you want to use.

   Valid port numbers are 23 or a port number from 9000 through 65355.

4. To change the TCP port for HTTP requests, in the **HTTP Port** field, enter the port number that you want to use.

   Valid port numbers are 80 or a port number from 9000 through 65535.

5. Click **Apply**.

## CLI Commands

Use the following command to change the TCP port for Telnet requests:

**ip telnet port <*tcp-telnet-port*>**

Use the following command to change the TCP port for HTTP requests:

**ip http port <*tcp-http-port*>**

*** Note:** You must be in Global Configuration mode and have administrative privilege to enter the **ip telnet port** and **ip http port** commands.

Use the following command to view the current TCP port settings for Telnet and HTTP:

**show tcp configuration**

*** Note:** You must have administrative privilege to enter the **show tcp configuration** command.

For more information about these commands, see Chapter 9, "IP," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*

### SNMP MIB Objects

Use the following MIB objects to change the TCP port for Telnet or HTTP requests. These MIB objects are located in **ProminetMib.txt**, version 5.2.

- .iso.org.dod.internet.private.enterprises.prominet.promPortMgmt.promTCPPortMgmt.promTCPPortHTTP
- .iso.org.dod.internet.private.enterprises.prominet.promPortMgmt.promTCPPortMgmt.promTCPPortTelnet

## Starting a Telnet Session

After changing the TCP port for Telnet requests to a port number other than 23, you must specify the TCP port number in addition to the IP address or host name to start a Telnet session.

For example, if you change the TCP port from 23 to 9998 on switch 192.168.0.126, enter **telnet 192.168.0.126 9998** to start a Telnet session.

For more information about the **telnet** command, see "telnet" in Chapter 30, "UI," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

## Opening the Web Agent

After changing the TCP port for HTTP requests to a port number other than 80, you must specify the TCP port number in addition to the IP address to open the Web Agent.

For example, if you change the TCP port from 80 to 9999 on switch 192.168.0.126, enter **http://192.168.0.126:9999** to open the Web Agent.

# Managing Configuration Files

When you first install the switch, or upgrade from a previous installation, your configuration parameters are stored in a **startup.txt** file located in the switch's Non-Volatile Random Access Memory (NVRAM). When the switch is restarted, the startup.txt file runs and stores configuration parameters in volatile RAM as a running configuration.

Any changes you make to the switch configuration are automatically recorded in RAM, but not in NVRAM. When you want to retain your current configuration, you must manually save it to NVRAM through the Web Agent or the CLI.

For information about how to save your running configuration file to your startup configuration, refer to the "Using the Web Agent", section later in this chapter. Always view and compare your running and startup configuration files to determine changes that you made to your running configuration.

You can manage the files that contain the configuration data for your multiservice switch from either the Web Agent or the CLI.

## Viewing Your Running Configuration

To view your running configuration:

- Select **Running Config** from the C**onfiguration Management** group on the Web Agent window. The **Running Configuration** dialog box displays

  Or

- Enter the following command in **Enable** mode from the CLI:

  ```
  ># show running-config
  ```

## Viewing Your Startup Configuration

To view your startup configuration:

- Select **Startup Config** from the **Configuration Management** group on the Web Agent window. The **Startup Configuration** dialog box displays

  Or

- Enter the following command in **Enable** mode from the CLI:

  ```
  >#show startup-config
  ```

## Viewing Your Script Execution Log File

Each time the startup.txt file or other script runs, a log file is generated. Log files contain the data returned from the script. You can view log file data from the Script Execution Log File using either the Web Agent or the CLI.

### Using the Web Agent

To view your Script Execution Log File from the Web Agent, select **Script Log File** from the **Configuration Management** folder on the Web Agent window. The **Script Execution Log file** displays

### Using the CLI

To view your Script Execution Log File from the CLI, enter the following command in **Enable** mode:

```
># show file_name logfile.txt
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Copying Configuration Files

If you make any changes, you must save the running configuration as the startup configuration to save the changes. Before you do this, always copy your startup configuration to a file on the switch or on a TFTP server.

You can save the running configuration to the startup configuration and copy the startup configuration to a file using either the Web Agent or the CLI.

*** Note:** Configuration files are automatically saved as text files using the *.txt extension on your switch.

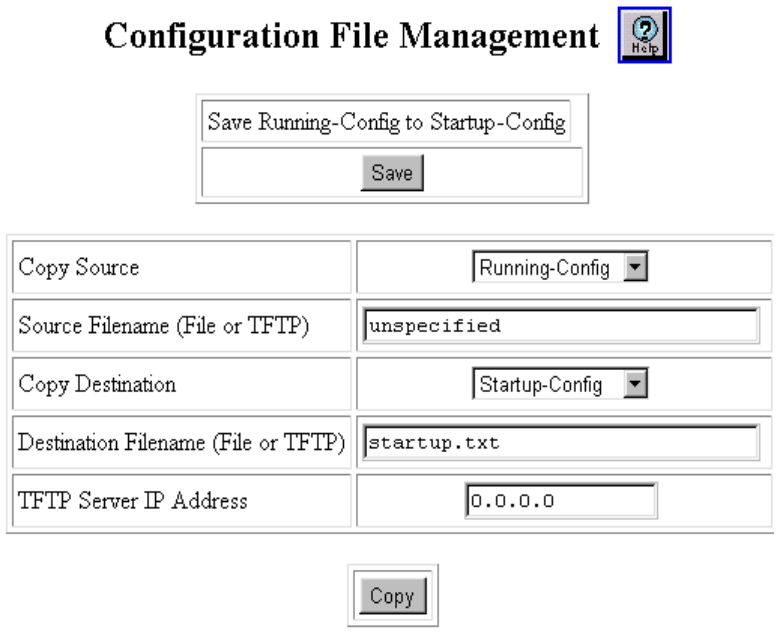
If you save the new file to a TFTP server, you can edit the startup.txt file using a text editor of your choice and save copies of it with a**.txt** extension.

## Using the Web Agent

To save your running configuration as your startup configuration in NVRAM using the Web Agent:

1. Select the **File Management** from the **System > Configuration > Configuration Files** group on the Web Agent window. The **Configuration File Management** dialog box opens (Figure 2-22).

***Figure 2-22. Configuration File Management Dialog Box - Partial***




2. Click **Save**. The running configuration is saved as the startup configuration.

*** Note:** You can also save the running configuration to the startup configuration through the Configuration File Management dialog box. Refer to the "Copying Files" section for that procedure.

### Using the CLI

To save your running configuration as your startup configuration in NVRAM using the CLI, enter the following command in **Enable** mode:

```
>#  copy running-config startup-config
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Copying Files

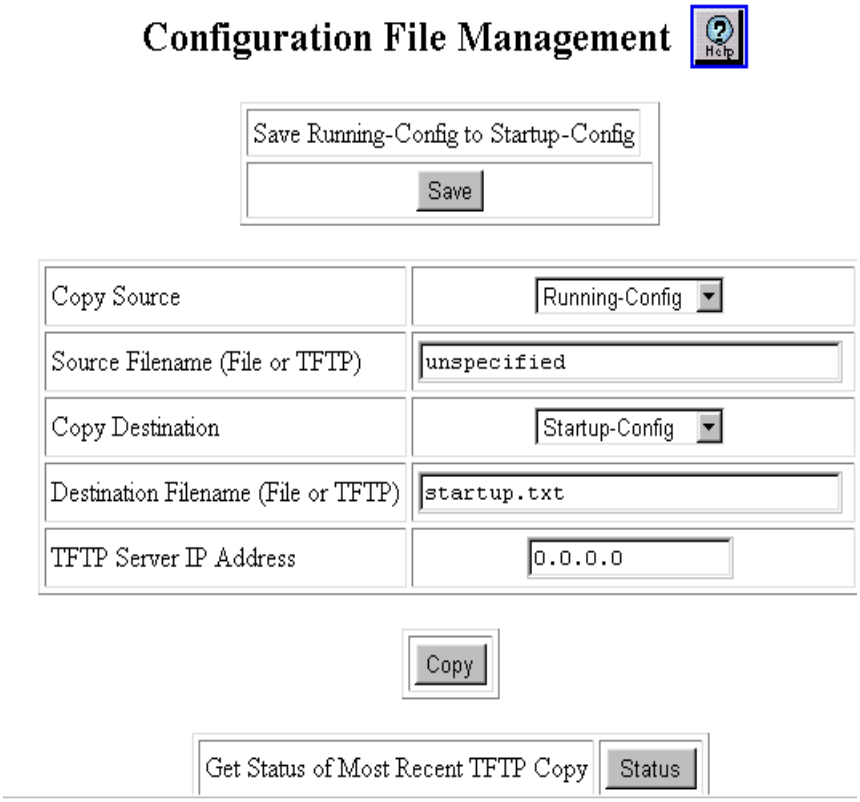
You can copy files to and from multiple locations. For example, if you modify the running configuration and you want to reinstate your startup configuration parameters, you can copy your startup configuration to your running configuration in volatile RAM. You can also upload or download configuration files by copying files from a TFTP server directory to the switch or to a startup or running configuration file. You can copy files using either the Web Agent or the CLI.

### Using the Web Agent

To copy files using the Web Agent:

1. Select File Management from the System > Configuration > Configuration Files group on the Web Agent window. The Configuration File Management dialog box opens (Figure 2-23).

*Figure 2-23. Configuration File Management Dialog Box*




**2.** Refer to Table 2-9 for an explanation of the Configuration File Management dialog box parameters.

*Table 2-9. Configuration File Management Dialog Box Parameters*

| Parameter | Description | Options |
|---|---|---|
| **Save Running-Config to Startup-Config** | Saves the running configuration to the startup configuration | N/A |
| **Copy Source** | Specifies the source file to be copied | • **Unspecified** - Specifies an initialized value.<br>• **File** - Specifies a source file located on the switch in NVRAM.<br>• **Running-Config** - Specifies a running configuration.<br>• **Startup-Config** - Specifies a startup configuration.<br>• **TFTP Server** - Specifies a source file located in a directory on a TFTP server. |

***Table 2-9. Configuration File Management Dialog Box Parameters** continued*

| Parameter | Description | Options |
|---|---|---|
| **Source Filename** | Specifies the path and name of the source file | Source files can be ASCII files in NVRAM available for upload or files located on a TFTP server available for download |
| **Copy Destination** | Specifies the location of the destination | • Unspecified- Specifies an initialized value.<br>• **File** - Specifies that a source is copied or downloaded to NVRAM.<br>• **Running-Config** - Specifies that a source is copied to the running configuration.<br>• **Startup-Config** - Specifies that a source is copied to the startup configuration.<br>• **TFTP Server** - Specifies that a source is copied to a TFTP server location. |
| **Destination Filename** | Specifies the path and name of the destination file | Configuration files and other files can be copied to NVRAM on the switch or to a TFTP server as a destination location. |
| **TFTP Server IP Address** | Specifies the IP address of a source or destination TFTP server | Copy (download) source files, located on a TFTP server, to your running configuration, your startup configuration, or a location on the switch. Or, copy (upload) your configuration files, or a file located on the switch, to a TFTP server. |

— File — To copy a file stored on the switch to your running or startup configuration, to a location on the switch, or to a location on a TFTP server.

— TFTP Server — To copy a file stored on a TFTP server to your running or startup configuration or to a file on the switch.

*** Note:** If you select File or TFTP Server, you must also provide the path and filename of the source file in the Destination Filename field.

3. Select one of the following from the Copy Destination pull-down menu.

   — **Running-Config** — Copies your startup configuration, or other file located on the switch or on a TFTP server, to your running configuration.

   — **Startup-Config** — Copies your running configuration, or other file located on the switch or on a TFTP server, to your startup configuration.

   — **File** — Copies your startup or running configuration, another file located on the switch, or a file located on a TFTP server to a file on the switch.

   — **TFTP Server** — Copies your startup or running configuration, or another file located on the switch, to a location on a TFTP server.

   *** Note:** If you select File or TFTP Server, you must also provide the path and filename of the destination file in the Source Destination field.

4. Enter the IP address of the source or destination TFTP server in the TFTP Server IP Address field, if applicable.

5. Click **Copy**. The source configuration or file is copied to your specified destination.

   *** Note:** The Web Agent returns an `Invalid operation!` error message if you attempt to copy one of the following:

   - The current running configuration to the running configuration.
   - The startup configuration to the same startup configuration.
   - The specified TFTP server to a TFTP server.

### Using the CLI

To copy files using the CLI, enter the following command in Enable mode:

```
>#  copy running-config +
```

*** Note:** Entering a "+" sign lists all of the applicable options for the `copy running-config` command

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Viewing the Status of a TFTP Transfer

After you have copied the startup configuration or other files to a TFTP server, you can use either the Web Agent or the CLI to check the status of the TFTP transfer to ensure that files copied correctly.

### Using the Web Agent

To view the status of a TFTP transfer using the Web Agent:

1. Select **File Management** from the **System > Configuration > Configuration Files** group on the Web Agent window. The **Configuration File Management** dialog box opens (Figure 2-23).
2. Select **Status** from the **Get Status of Most Recent TFTP Copy** field. A status message displays in the **Config File Mgmt Status** window.

### Using the CLI

While doing a TFTP transfer using the CLI, the status, either successfully transferring or an error condition, is immediately returned.

*** Note:** You cannot view the status of a TFTP transfer done using the CLI from the Get Status of Most Recent TFTP Copy field on the Web Agent.

```
> show startup-config
```

# 3 Configuring System Information

## Overview

You can manage system information by using either the Web Agent or the CLI. The following procedures to manage your system information are provided in this chapter:

- Entering General System Information
- Enabling the Simple Network Time Protocol
- Setting Summer Time Hours
- Setting the System Clock
- Setting the Temperature System
- Displaying the Power System Statistics
- Displaying Cooling System Statistics
- Performing a Reset

*** Note:** The last step in each procedure tells you to click Apply to save any changes. This saves the changes to the Running config only. The Startup config has not changed. Therefore, these and other changes will be lost if your switch goes down or if you power off.

To save these changes to the Startup Config, you must copy the Running config to the Startup config. Refer to the "Copying Files," in Chapter 2, *"Initialize and Setup"*.

## Entering General System Information

You can enter general information about your system by using either the Web Agent or the CLI.

### Web Agent Procedure

You can enter general system information using the following Web Agent fields:

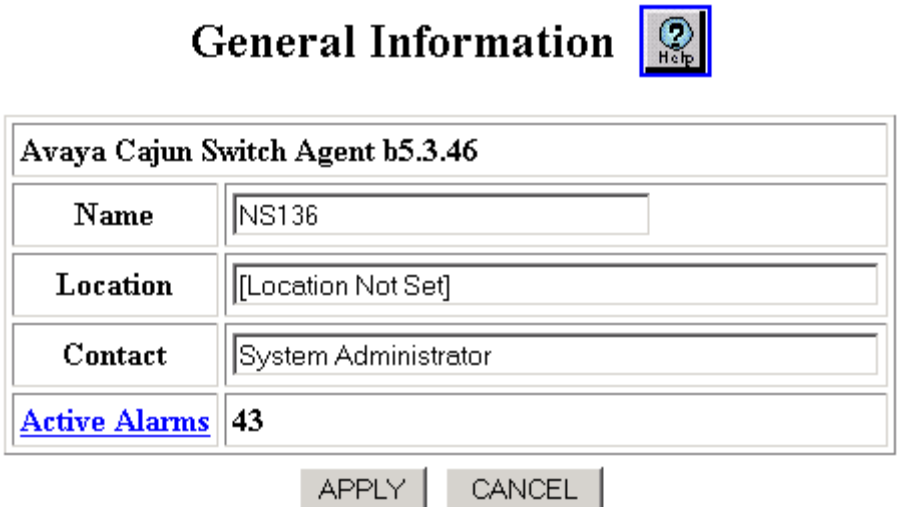
- Switch name

- Device location
- Device contact

To enter general system information from the Web Agent:

1. Select General Information from the System group on the Web Agent window. The General Information dialog box opens (Figure 3-1).

*Figure 3-1. System Information Window*




2. Enter the switch name in the Name field.
3. Enter the location for the switch (for example, floor, closet in the Location field.
4. Enter the person who should be contacted in the event of a problem in the Contact field.
5. Click APPLY to save your changes, or CANCEL to clear your selection.

# Enabling the Simple Network Time Protocol

You can enable Simple Network Time Protocol (SNTP) on your switch using either the Web Agent or the CLI. Enabling SNTP automatically synchronizes time on all computers, switches, and other devices connected to your switch.

When you enable SNTP, you are required to set your time zone and the rule or dates of Summer Time Hours for your location. For information about setting one-time summer hours, refer to “Setting

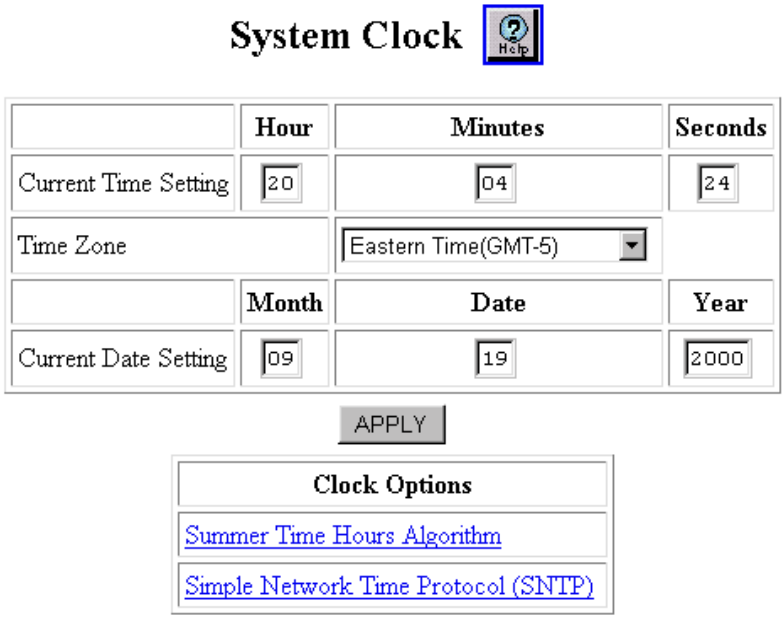
One-Time Summer Time Hours" later in this chapter. For information about setting Summer Time Hours, refer to "Setting Summer Time Hours" later in this chapter.

## Web Agent Procedure

To enable SNTP on your switch using the Web Agent:

1. Select System Clock from the System > Configuration group on the Web Agent window. The System Clock dialog box opens (Figure 3-2):

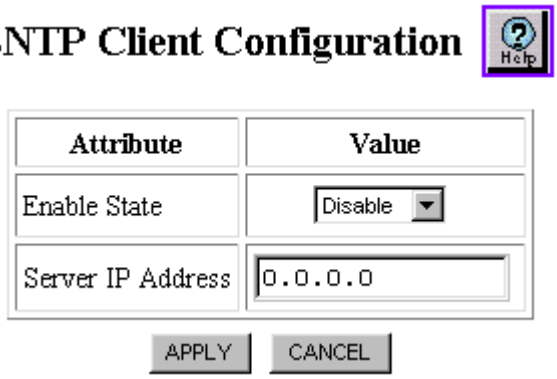
***Figure 3-2. System Clock Dialog Box.***




2. Select Simple Network Time Protocol (SNTP) from the Clock Options box. The SNTP Client Configuration window opens (Figure 3-3).

***Figure 3-3. SNTP Client Configuration Dialog Box***

3. Select Enable from the Enable State pull-down menu. The default is Disable.
4. Enter the server IP address in the Server IP address field for the switch on which you want to enable SNTP.
5. Click APPLY to save your changes, or CANCEL to clear your selection.




### CLI Command

To enable SNTP on your switch using the CLI, enter the following command in Configure mode:

```
> <configure># sntp server <ip-address>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Beta Version 5.3* for details about this command.

# Setting Summer Time Hours

Summer Time Hours, also referred to as Daylight Savings Time (DST), is the strategy of moving clocks ahead to provide greater amounts of daylight in the afternoon and to standardize time with other parts of the world. In many parts of the world, the Summer Time Hours algorithm is based on a standardized rule. For example, in the Western hemisphere, the rule used by most locations in Canada, Mexico, and the United States is to set clocks forward by one hour at 2:00 a.m. on the first Sunday in April and back an hour at 2:00 a.m. on the first Sunday in October annually. Many countries in Europe and Asia follow similar rules. The offset, or amount of time by which the clock is set forward or backward, varies from country to country.

Many parts of the world follow a one-time change of Summer Time Hours. When you configure the switch for these locations, you reset the clock by specifying a scheduled time and date.

This section provides the following procedures:

- Setting Recurring Summer Time Hours
- Setting One-Time Summer Time Hours

*** Note:** If you upgrade your switch from a previous version, the local time settings are saved as Greenwich Mean Time values. Always change the Summer Time Hours Algorithm before you set the clock.

## Setting Recurring Summer Time Hours

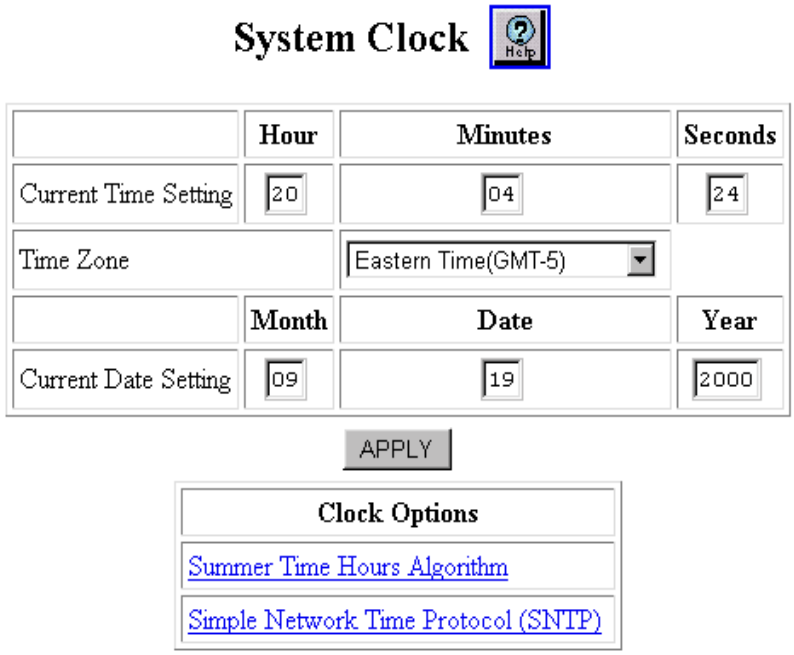
You can set recurring summer time hours using either the Web Agent or the CLI.

### Web Agent Procedure

To set recurring Summer Time Hours using the Web Agent:

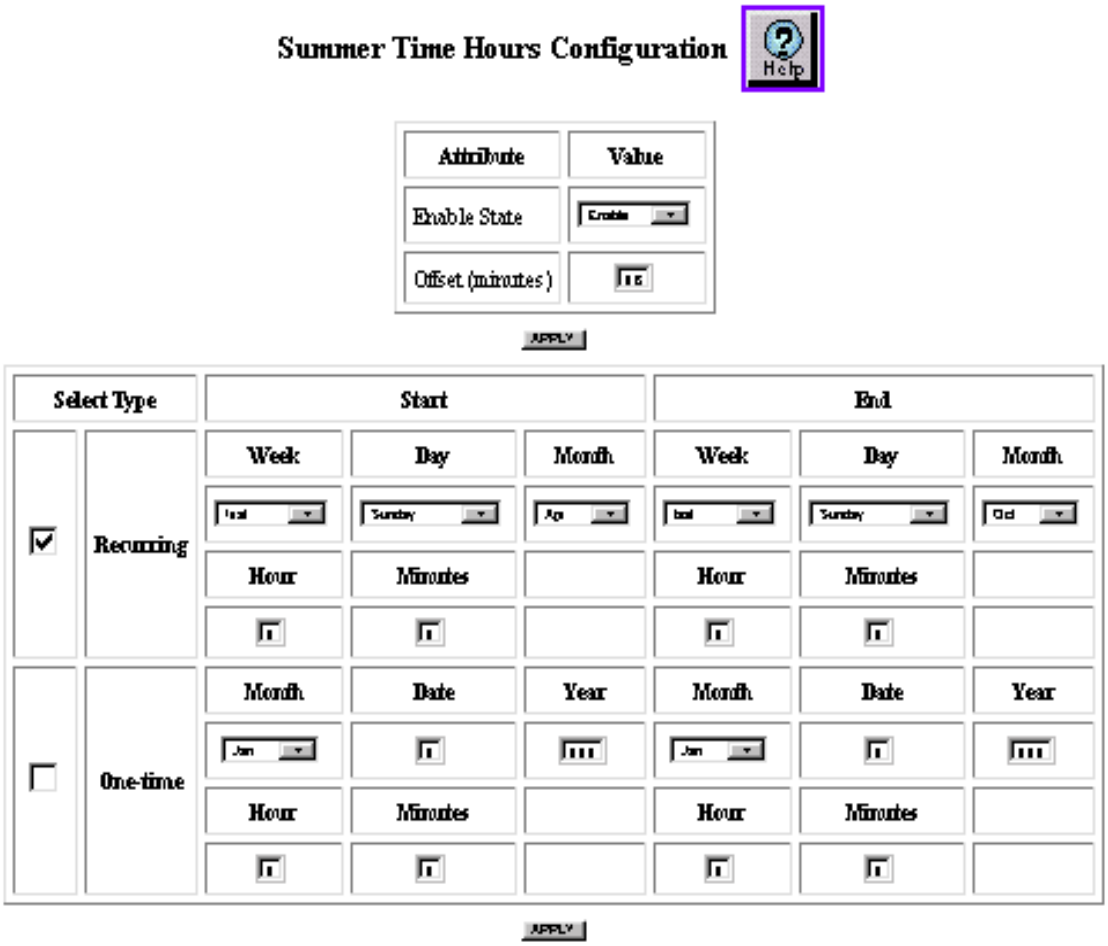
1. Select System Clock from the System> Configuration group on the Web Agent. The System Clock dialog box opens (Figure 3-4).

***Figure 3-4. System Clock Dialog Box***




2. Select Summer Time Hours Algorithm from the Clock Options field. The Summer Time Hours Configuration dialog box opens (Figure 3-5).

*Figure 3-5. Summer Time Hours Dialog Box*




3. Select **Enable** from the **Enable State** pull-down menu.

4. Enter the reset value for the clock in minutes in the **Offset** field. For example, if you intend to reset the clock forward or backward by one hour, keep the default value of 60 minutes.

5. Set the Summer Time Hours that recur annually:

   a. Select the check box in the **Recurring** field.

   b. Select the values for the **Week**, **Day**, and **Month** when the Summer Time Hours are to start and end.

   c. Enter values for the **Hour** and **Minutes** when Summer Time Hours are to start and end.

6. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

Refer to Table 3-1 for detailed information about the fields in the Recurring Summer Time Hours section of the Summer Time Hours Configuration dialog box.

***Table 3-1. Recurring Summer Time Hours Parameters***

| Parameter | Definition |
|---|---|
| **Recurring** | Select if the Summer Time Hours option is defined by a rule such as Daylight Savings Time (DST - all Start and End fields associated with Recurring Summer Time Hours provide the default values for DST).<br>When you select the Recurring Summer Time Hours option, indicate the time, in hours and minutes, on a specified day, week, and month that you want the Summer Time Hours begin and end. |
| **Start** | Specifies the start of Summer Time Hours. |
| **End** | Specifies the end of Summer Time Hours. |
| **Week** | Select the week during which you want recurring Summer Time Hours to start or end. The selected week should reflect the day on which Summer Time Hours start. For example, if Summer Time Hours start on the first Sunday in April, select the First week. Options include:<br>• **First -** First week of the month, the default Start value, when Daylight Savings Time starts in the Western hemisphere.<br>• **Second -** Second week of the month.<br>• **Third -** Third week of the month.<br>• **Fourth -** Fourth week of the month.<br>• **Last -** Remaining days of the month that form the last week of the month. Last is specified as the default End value, denoting when Daylight Savings Time ends in the Western hemisphere. |

*Table 3-1. Recurring Summer Time Hours Parameters continued*

| Parameter | Definition |
|---|---|
| **Day** | Select the day of the week when you want recurring Summer Time Hours to start or end. Options are based on a seven-day week and include:<br>• **Sunday -** the default Start and End values. In the Western hemisphere, DST starts on the first Sunday in April and ends on the last Sunday in October.<br>• Monday<br>• Tuesday<br>• Wednesday<br>• Thursday<br>• Friday<br>• Saturday |
| **Month** | Select the month when recurring Summer Time Hours start or end. The twelve months of the Gregorian calendar are provided.<br>For recurring Summer Time Hours, the default Start value is April, the month during which DST starts in the Western hemisphere. The default End value is October, the month during which DST ends in the Western hemisphere. |
| **Hour** | Enter a value to represent the hour when Summer Time Hours start or end for Recurring settings.<br>For Recurring Summer Time Hours, the default value is 02, meaning 2:00 a.m., for both Start and End hours. |
| **Minutes** | Enter a value to represent the number of minutes into the hour when Summer Time Hours start or end for Recurring Summer Time Hours. The default value is 00 for both Start and End minutes. |

## CLI Command

To set recurring Summer Time Hours using the CLI, enter the following command from Configure mode:

```
<configure># clock summer-time recurring <week>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Beta Version 5.3* for details about this command.

# Setting One-Time Summer Time Hours

You can set one-time summer time hours using either the Web Agent or the CLI.

## Web Agent Procedure

To set Summer Time Hours that are not based on a standard rule using the Web Agent:

1. Select System Clock from the System> Configuration group on the Web Agent window. The System Clock dialog box opens (Figure 3-4).
2. Select Summer Time Hours Algorithm from the Clock Options field. The Summer Time Hours Configuration window opens (Figure 3-5).
3. Select Enable from the Enable State pull-down menu. The default is Disable.
4. Enter the reset value for the clock in minutes in the Offset field. For example, if you intend to reset the clock forward or backward by one hour, keep the default value of 60 minutes.
5. Select the check box next to the One-Time field to set the date and time for Summer Time Hours on a one-time basis:
   a. Enter the specific Month, Day, and Year when the Summer Time Hours start and end.
   b. Enter the Hour and Minutes when the Summer Time Hours start and end.
6. Click APPLY to save your changes, or CANCEL to clear your selection.

Refer to Table 3-2 for detailed information about the One-Time field parameters for the Summer Time Hours Configuration dialog box.

***Table 3-2. One-Time Summer Time Hours Configuration***

| Parameter | Definition |
|---|---|
| **One-time** | Select if Summer Time Hours change one time, such as on a specified date.<br>When you select one-time Summer Time Hours, you indicate the time and date on which Summer Time Hours begin and end. |
| **Start** | Specifies the start of Summer Time Hours. |
| **End** | Specifies the end of Summer Time Hours. |

### CLI Command

To set Summer Time Hours that are not based on a standard rule using the CLI, enter the following command from Configure mode:

```
<configure># clock summer-time date
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Beta Version 5.3* for details about this command.

# Setting the System Clock

The system clock is used for setting traps, alarms, and other events on the switch.

*** Note:** You must set SNTP and Summer Time Hours before you can set the system clock. Refer to "Enabling the Simple Network Time Protocol" and "Setting Summer Time Hours" earlier in this chapter.

The system clock does not automatically change with Daylight Savings Time.

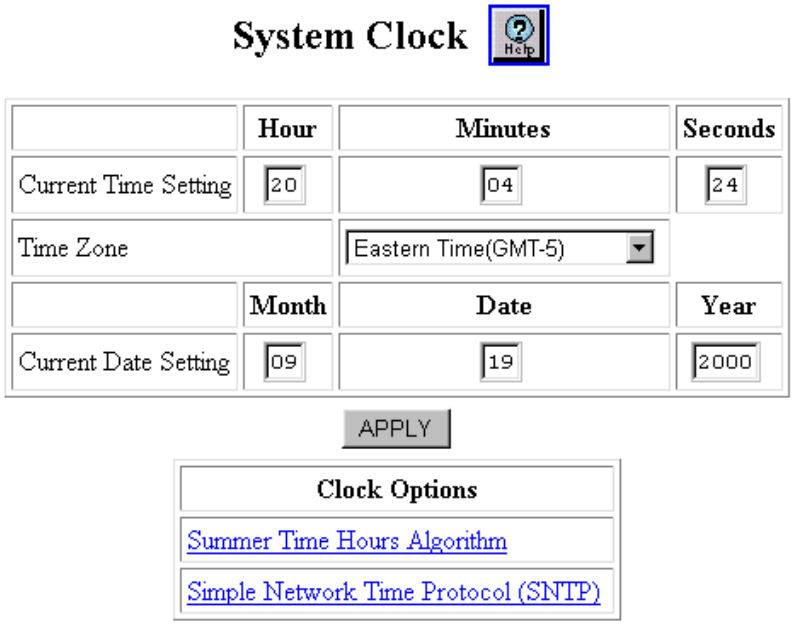
You can set the system clock from either the Web Agent or the CLI.

### Web Agent Procedure

To set the system clock using the Web Agent:

1. Select System Clock from the System > Configuration group on the Web Agent window. The System Clock dialog box opens (Figure 3-6).

*Figure 3-6. System Clock Dialog Box*




2. Enter the time in the **Current Time Setting** Hour, Minutes, and Seconds fields using 24-hour time format (for example, 10 p.m. is 22:00 00.
3. Select the time zone for your area from the **Time Zone** pull-down menu.
4. Enter the current Month, Date, and Year in the **Current Date Setting** fields.
5. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

## CLI Command

To set the system clock using the CLI, enter the following command from User mode:

```
> clock set <time> <date> <year>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Beta Version 5.3* for details about this command.

# Setting the Temperature System

You can set the upper and lower temperature warning systems for your switch's backplane and slot 1. These warning systems cause the following to happen if the temperatures you set are reached:

- The Supervisor modules shut down the switching modules if the temperature reaches the Shutdown temperature.
- The modules are restarted if the temperature goes below the Upper Warning Temperature.

The default Shutdown temperatures are conservative for the slot 1 sensor (50° C and backplane sensor 50° C). They can be safely set to 60° C, but settings higher than 60° C are not recommended. You can set the shutdown temperature to a value lower than 50° C to ensure prompt notification if a fan fails.

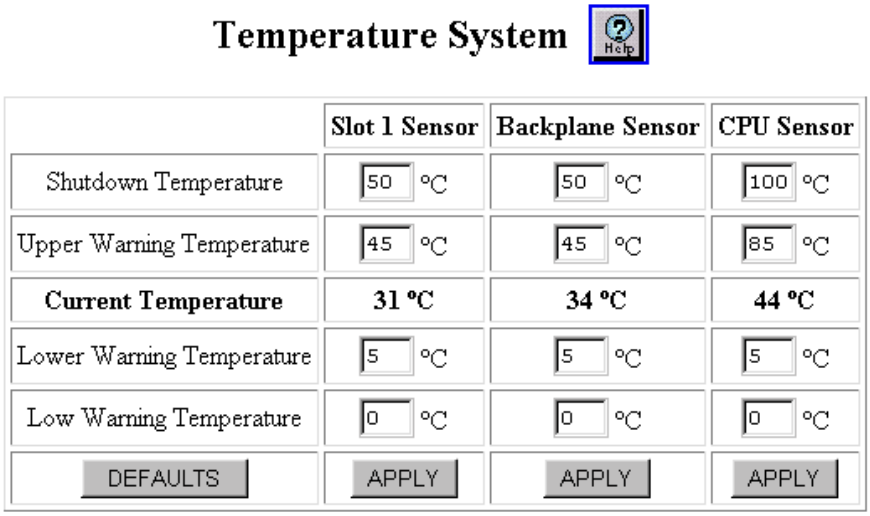
You can set the temperature system using either the Web Agent or the CLI.

## Web Agent Procedure

To configure the temperature warning systems using the Web Agent:

1. Select **Temperature System** from the **System > Configuration** group on the Web Agent window. The **Temperature System** dialog box opens with the current temperature settings (Figure 3-7).

*Figure 3-7. Temperature System Window*




2. Enter your desired temperature warnings in the **Slot 1 Sensor**, and the **Backplane Sensor** fields.

   *** Note:** "Slot 2" will display if the only sensor supervisor is in slot 2.

3. Enter a temperature warning in the **CPU Sensor** field.

4. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

### CLI Command

To configure the temperature warning systems using the CLI, enter the following command from Configure mode:

```
<configure># set temperature <backplane-sensor>
<cpu-sensor> <probe> <supervisor-slot>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Beta Version 5.3* for details about this command.

# Displaying the Power System Statistics

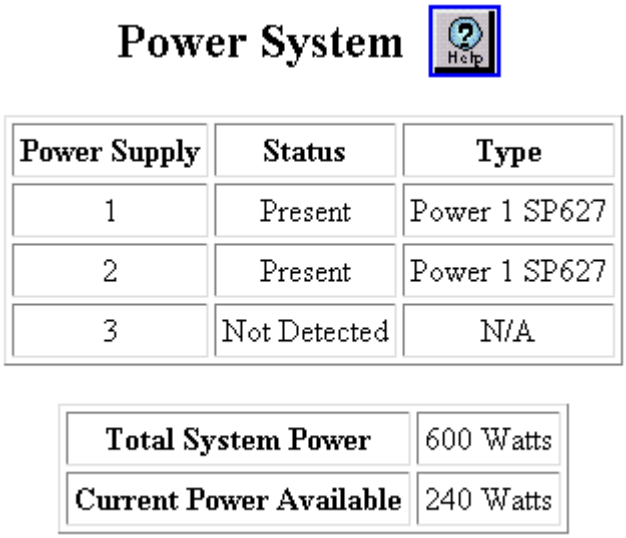
You can display the statistics for your switch's power system from the either the Web Agent and the CLI.

### Web Agent Procedure

To display your switch's power system statistics using the Web Agent:

1. Select **Power System** from the **System>Configuration** group on the Web Agent window. The **Power System** dialog box opens with your switch's current power statistics (Figure 3-8).

*Figure 3-8. Power System Window*




2. Refer to Table 3-3 and review the **Power System** dialog box parameters:

*Table 3-3. Power System Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Power Supply** | Identifies the power supply |
| **Status** | indicates whether the power supply is detected. |
| **Type** | Describes the type of power supply detected. |
| **Total System Power** | Displays the total system power in Watts. |
| **Current Power Available** | Displays the current power available. |

*** Note:** You will see 1400W of available power displayed in the **Total System Power** field if you have three power supplies installed. The switch only uses power from two of the three power supplies. The third power supply is a redundant power supply and is used only if one of the other power supplies fails.

## CLI Command

To display your switch's power system statistics using the CLI, enter the following command from the User mode:

```
> show system power
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Beta Version 5.3* for details about this command.

# Displaying Cooling System Statistics

You can display the statistics for your switch's cooling system from either the Web Agent or CLI.

## Web Agent Procedure

To display your switch's cooling system statistics using the Web Agent:

1. Select **Cooling System** from the **System > Configuration** group on the Web Agent window. The **Cooling System** dialog box opens with the status of your switch's cooling system (see Figure 3-9 for the P550R/P580 switch, or Figure 3-10 for the P880 and P882 switch).

***Figure 3-9. P550R/P580 Cooling System Status Window***

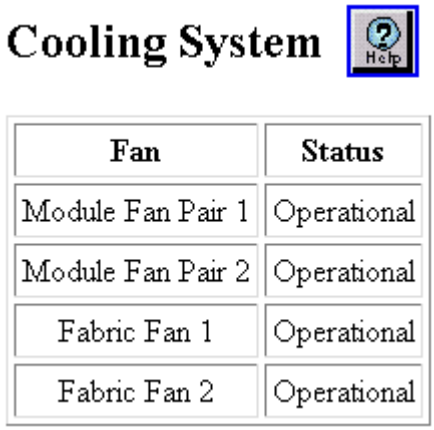
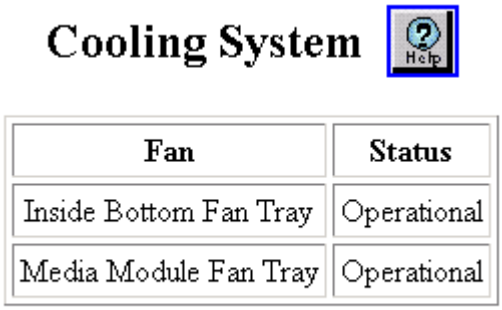


*Figure 3-10. P880/P882 Cooling System Status window*




2. Check the Status column to ensure that all the individual components are operational.

3. If a component's status is non-operational, power down the switch and contact a service representative to diagnose the failing unit.

### Using the CLI

To display your switch's power system statistics using the CLI, enter the following command from **Configuration** mode:

```
<configure># show system fans
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Beta Version 5.3* for details about this command.

# Performing a Reset

You can reset your switch from either the Web Agent or the CLI.

*** Note:** You must reset your switch after licensing an 80-Series modules.

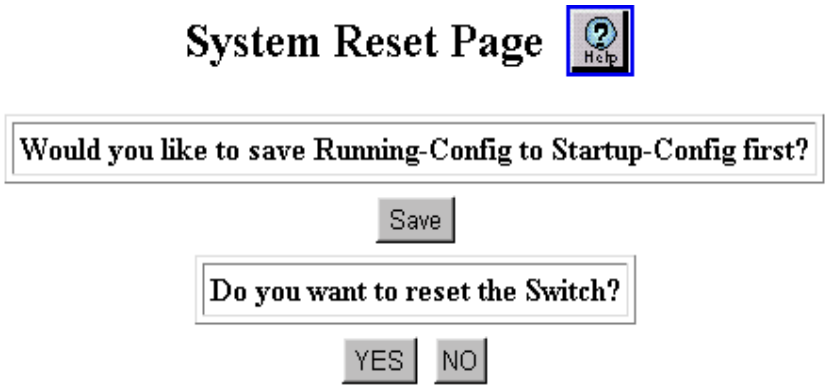
### Using the Web Agent

To reset your switch using the Web Agent:

*** Note:** You can also reset your switch using the **Module Reset** button located on the Supervisor module. Refer to the Installation Sheet that came with the Supervisor Module for details.

1. Select **System Reset** from the **System** group on the Web Agent window. The **System Reset Page** dialog box opens (Figure 3-11).

*Figure 3-11. System Reset Page Window*




2. Select **Save** to save your Running Configuration (Running-Config to the startup configuration (Startup-Config before performing a system reset.

   *** Note:** If you do not save your Running-Config to Startup-Config before you reset the switch, you will lose all of the modifications you made.

3. Click YES to reset the switch, or NO to cancel the operation.

## CLI Command

To reset your switch using the CLI, enter the following command from Priv mode:

```
# reset
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Beta Version 5.3* for details about this command.

## SNMP

To reset the switch remotely by using SNMP, use the MIB object that is listed in Table 1.

*** Note:** You must have administrative privilege to perform this task.

*Table 1. MIB, MIB Object, and OID for Remotely Resetting the Switch*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.2 | promChassisSystemReset | 1.3.6.1.4.1.2167.3.1.3 |

# 4 Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping

## Overview

The following information and procedures are provided in this chapter and pertain to layer 2 and layer 3 module configurations:

- VLAN Introduction
- Creating and Implementing VLANs
- Spanning Tree Protocol Setup and Monitoring
- Using Hunt Groups to Aggregate Bandwidth between Switches
- Configuring VLAN Trunk Protocol (VTP) Snooping

## VLAN Introduction

This section introduces Virtual Local Area Networks (VLANs), explains how they operate, and provides procedures for creating VLAN's.

### Need for VLANs

If a traditional bridge receives a frame with a broadcast, multicast, or unknown destination address, it forwards the data to all bridge ports except the port on which it was received. This process is referred to as bridge *flooding*. As networks grow and the amount and types of traffic increase, bridge *flooding* may create unnecessary traffic problems that can clog the Local Area Networks (LAN).

To help control the flow of traffic through a switch and meet the demands of growing networks, vendors have responded by using:

- Customized packet filtering to control which packets are forwarded.
- More routers as broadcast firewalls to divide the network into broadcast domains.
- Spanning Tree Protocol to control the flow of traffic among LANs (for redundant links).

Advantages with VLANs:

- Segment traffic and usage patterns in a manner similar to creating subnets and segments in traditional networks.
- Reduce the cost of equipment moves, upgrades, and other changes.
- Simplify network administration.
- Create logical workgroups for users who share the same system resources.
- Users not required to share the same physical location.
- Reduce the need for routing to achieve higher network performance and reduced costs.
- Control or filter communication among broadcast domains.

# What is a VLAN?

The Avaya Multiservice Switch has the ability to create separate logical LANs on the same physical device. These logical segments are referred to as Virtual LANs (VLANs).VLANs are typically groups of users with similar job functionality (i.e. sales, marketing, engineering etc.) and share common resources. VLANs are not constrained by their physical location and can communicate as if they were on a common LAN. VLAN members can reside on single or multiple ports on one or more media modules on a switch, or on different switches. VLANs are limited broadcast domains, meaning all members of a VLAN receive every broadcast packet seen by members of the same VLAN, but not packets sent by members of a different VLAN. A router is required when communicating between different VLANs.

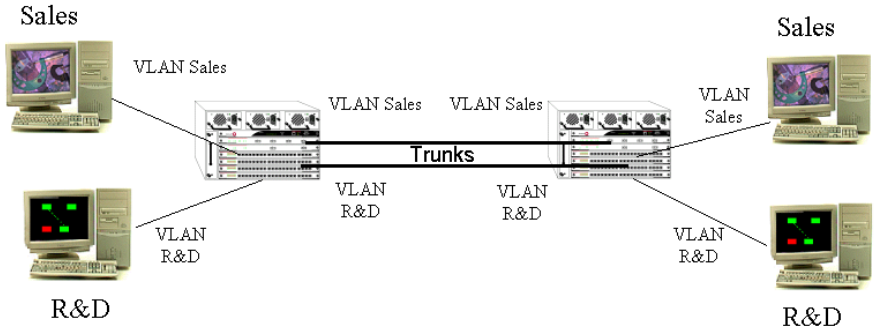
## Port Based VLANS

The Avaya Multiservice switch is a Port Based VLAN architecture. VLAN membership is defined by groups of switch ports. When a VLAN is created three types of information is configured for that VLAN, the VLAN name, the VLAN Identifier or VLAN ID, and the switch ports assigned to that VLAN. VLAN assignment of a packet is based on a global VLAN ID. Regardless of any name you assign to a VLAN, the switch looks only at the VLAN ID number to determine a packet's VLAN destination.

For example, ports 1, 2, and 3 on a module are members of VLAN A, ports 4, 5, and 6 on another module are also members of VLAN A. Traffic is forwarded through the switch to all ports that are members of VLAN A.

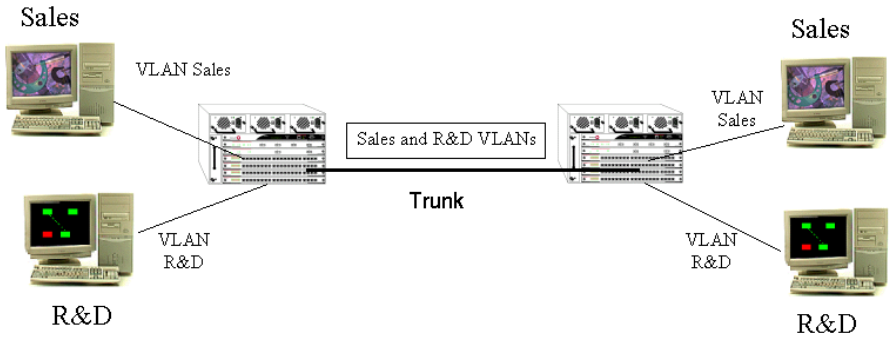
A switch that is strictly port based needs additional information to separate traffic passing from one VLAN to another. Since each port is dedicated to a particular VLAN, there is no need to analyze the traffic arriving on a port to determine its VLAN membership. As an example, (Figure 4-1) two switches with two VLANs, Sales and R&D, would need a dedicated switch to switch connections (Trunk) for both VLANs between switches. Therefore all traffic arriving on that port must belong to the VLAN assigned to that port since, in this case, no unique identifiers are sent with the frames.

***Figure 4-1. Vlans No Tagging***




The Avaya Multiservice switch is able to separate VLAN traffic between switches across a single Trunk links. In order to accomplish this, the switch implements VLAN Tagging and Trunking. VLAN Tagging is enabled on a switch port by selecting a Trunk mode for that port; clear, IEEE 802.1Q or Cisco-Multi Layer mode. A trunk port can send frames in clear mode, with no VLAN ID, or the VLAN ID, over the same trunk. A frame is classified as belonging to a particular VLAN based on the value of the VLAN Identifier (VID) that is included in the Tag Header. Therefore using our example, and implementing VLAN tagging, we need only one connection (trunk) between the two switches to carry the traffic from both VLANs.(Figure 4-2)

*Figure 4-2. VLANs with 802.1Q tagging*




## IEEE 802.1Q VLAN Tagging

The Avaya Multiservice switch is compliant with the IEEE 802.1Q standard for VLANs and defines a Tag Header. Two Tag formats are defined as an Ethernet Encoded (4 bytes) for 802.3 and Ethernet V2 and SNAP (Service Network Access Point) for Token Ring and Fiber Distributed Data Interface (FDDI).

The Ethernet version of the Tag Header consists of 4 bytes, two bytes for Tag Protocol ID and two bytes for Tag Control. The Tag Protocol ID bytes contain an Ethernet Type value of 81-00 which identifies the frame as a tagged frame. The Tag Control specifies tag formats that are used to embed explicit VLAN membership information within each frame in a 12-bit VID that provides 4094 possible VLAN ID's. IEEE 802.1Q defines the bridging rules for VLANs (ingress and egress rules which are described in detail in the "VLAN Operation" section later in this chapter).

## VLAN Operation

VLAN operation is based on three sets of rules:

- Ingress Rules
- Forwarding Rules
- Egress Rules

# Ingress Rules

Every frame received by the switch is classified to one VLAN. There are two ways in which frames are classified to VLANs:

- Untagged frames are classified to the VLAN associated with the port on which the frame is received (Port-based VLANs).

- Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame.

  ***Note:** The switch supports a feature called **Automatic VLAN Creation** for tagged frames. For more information, refer to "VLAN Considerations" on page 7 for more information.

## Forwarding Rules

These rules determine the set of ports on the switch through which members of the VLAN can be reached. This is called binding a port to a VLAN. A port may be bound to a VLAN using four methods:

- Setting the **Port VLAN** attribute in the Switch Port Configuration web page.This identifies the VLAN to which all untagged frames received on the port are forwarded. **Static Binding**, the port is bound to the VLAN selected in the Port VLAN parameter.

  ***Note:** A port has one **Port VLAN**. Changing this to a new VLAN removes the port from the old VLAN.

- Setting the **VLAN Binding** attribute in the Switch Port Configuration dialog box to **Bind to All** should be done on links connecting two layer2 switches, where multiple VLANs span across both switches, such that members of each VLAN are found on both sides of the link. Bind-to-all should not be used when the switches on both ends of the link act as routers, such that each IP subnet and each VLAN are confined to one side of the link only and do not have members connected to the switch at the other end. In such routing cases, the link is never used for intra-VLAN traffic but rather is used only for traffic routed from one router to the other. Thus, there is no need for the link to belong to multiple VLANs, and should not be configured to bind-to-all. It should be bound to a single VLAN that is dedicated to the connection between the two routers. Bind-to-all in this case is not only unnecessary, but also undesired as a lot of irrelevant broadcast/multicast traffic of other VLANs will be sent onto this link and into the switch on the other end, unnecessarily increasing the control-plane load on the supervisor and increasing the chance for harmful layer3 configuration errors.

- Setting the **VLAN Binding** attribute in the Switch Port Configuration dialog box to **Bind to Received**. This causes the port to be bound to all VLANs (as identified by the VLAN tag in tagged frames) received on this port. Consequently, ports are bound to those VLANs that actually have members that are reachable through the port.
- When an untagged frame arrives on a port that is set to **Bind to ALL,** it forwards the frame to the "port VLAN". When a tagged 802.1Q frame arrives on a port that is set to **Bind to All** and the VLAN doesn't exist on the switch the frame is dropped.

**Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame.

**Forwarding**: Only forward frames to the port for the assigned VLAN.

**Egress:** All frames transmitted out of the port to be tagged using the IEEE 802.1Q/Multi-Layer tag header format. The tagged used will be that assigned to the port.

## Binding a Port to more than one VLAN using the CLI

A port can be statically configured to Bind to more than one VLAN. This causes the port to become a member of each specified VLAN. This feature is configured from the CLI. This feature cannot be configured from the Web Agent.

To configure from the CLI enter the following command:

```
<configure># set VLAN {<VLAN-id> | name <VLAN-name>}
<mod-swport-range>[...,<mod-swport-range>]
```

**CAUTION**

This configuration should only be used under special circumstances and with the assistance of customer support.

*** Note:** The Web Agent does not allow static binding of multiple VLANs to a single port. If you use the CLI to statically bind multiple VLANs to a single port, do not attempt to use the Web Agent to statically bind additional VLANs to the port or remove existing VLANs from the port.

## Egress Rules

For a given port/VLAN combination, egress rules determine whether frames transmitted from the port on the VLAN are tagged or untagged. This is accomplished by setting the Trunking Mode attribute in the Switch Port Configuration web page.

For example, choosing the IEEE 802.1Q trunk mode causes all frames transmitted out of the port to be tagged using the IEEE 802.1Q tag header format. Individual port/VLAN combinations may be changed to cause frames transmitted from the port to be untagged (or clear mode).

# Creating and Implementing VLANs

Adding users to VLANs include:

- VLAN Considerations
- Creating a VLAN
- Assigning Ports to VLANs

## VLAN Considerations

Be aware of the following issues when configuring VLANs:

- If multiple VLANs are statically bound to a port and you change the setting of the **Port VLAN** field on the Switch Port Configuration Web page, the switch may erroneously remove one or more of the VLANs from the port.
- If you set **Trunk Mode** to **Clear**, you must set the **VLAN Binding Type** to **Static** (default).
- The switch supports a feature called **Automatic VLAN Creation** for tagged frames. When this feature is enabled, the switch creates new VLANs when it receives packets from previously unknown VLANs. Vlan's can be created automatically without manually creating the VLAN on each switch.
- **Automatic VLAN Creation** does not work on an 80-series supervisor module (M8000R-SUP) if the **Port default VLAN** is set to **discard**.
- If you enable **"AUTOMATIC VLAN CREATION"** AND set "VLAN Binding" type to **Bind to Received**, make sure that you set the binding type before enabling **"AUTOMATIC VLAN CREATION"OR** else the port may not be automatically added to the VLAN.

- Assigning one of the ports of a 48-port module to a VLAN for which there exists IP interface will force that interface to be in the UP state, even when there is no physical connection to the module.

## Creating a VLAN

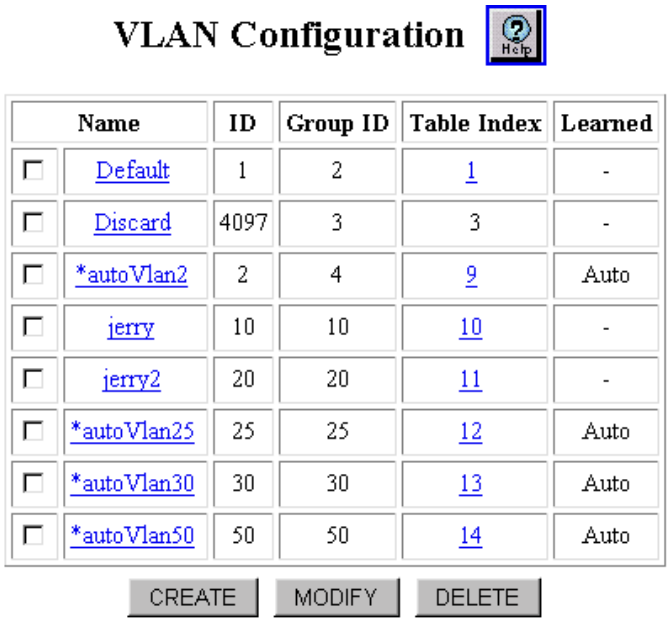
**CAUTION**

**Before creating or adding additional VLANS, it is Strongly Recommended to review the contents of Chapter 4** *Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping***, and Chapter 6,** *Managing the Address Forwarding Table***.**

To create a VLAN:

1. Select **Configuration** from the **L2 Switching > VLANs** folder on the Web Agent window. The **VLAN Configuration** dialog box opens (Figure 4-3).

***Figure 4-3. VLAN Configuration Dialog Box***



2. Click **CREATE**. The **Create VLAN** dialog box opens (Figure 4-4).

*Figure 4-4. Create VLAN Dialog Box*

3. Enter a name for the VLAN in the **Name** field.

4. In the ID field, enter an unused VLAN ID value (between 2 to 4094).

   VLAN IDs are global and must be consistent from switch to switch, even when switches are manufactured by different vendors.

5. Refer to Table 4-1 to configure the **Create VLAN** dialog box parameters:

*Table 4-1. Create VLAN Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Name** | Unique Name assigned to the VLAN in a switch. A maximum of 31 alphanumeric characters |
| **ID** | Identifier used throughout the network to identify this VLAN. If you want ports on more than one device to participate in a particular VLAN, you must use the same VLAN ID to identify the VLAN on every device.VLAN ID 1 is reserved for the Default VLAN. VLAN ID 4097 is reserved for the discard VLAN.<br>**Note:** The switch supports up to 1000 VLANs and a maximum of 24,000 MAC Addresses.<br>**Note:** In order to support the maximum number of VLANs, VLAN ID numbers should be chosen from the range of 1 to 1000. |

*Table 4-1. Create VLAN Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Initial Hash Table Size** | For every VLAN created, a hash table is allocated of the initial size. The hash table keeps track of the Layer 2 (MAC) addresses associated with a VLAN.<br>The default setting for *Initial Hash Table Size*,1024, allows the user to configure approximately 20 simultaneous VLANs. However, the switch supports 1,000 VLANs. To support 1000 simultaneous VLANs, the Hash table size should be at 16. To increase the number of VLANs you can implement, simply decrease the initial hash table size for each new address table instance.<br>**Note:** The number of addresses for a given hash table is approximately 4:1 (for example, if you have a hash table of 6 bytes, the VLAN can hold 64 addresses in it's table instance. |
| **Auto Increment HT Size** | *"Auto-Increment HT (Hash Table) Size"* determines whether the size of the VLAN's Hash Table can grow if software determines it to be undersized for the number of known Layer 2 addresses of a VLAN. Select "true" to allow the switch to increase the size of the Hash Table. Select "False" to disable the feature. The default is "True". |

6. Click **APPLY** to create the new VLAN, or **CANCEL** to restore previous settings.

**CAUTION**

**Before configuring Hash Tables and Auto Increment Hash Table parameters, it is Strongly Recommended to review the contents of Chapter 4** *Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping***, and Chapter 6,** *Managing the Address Forwarding Table***.**

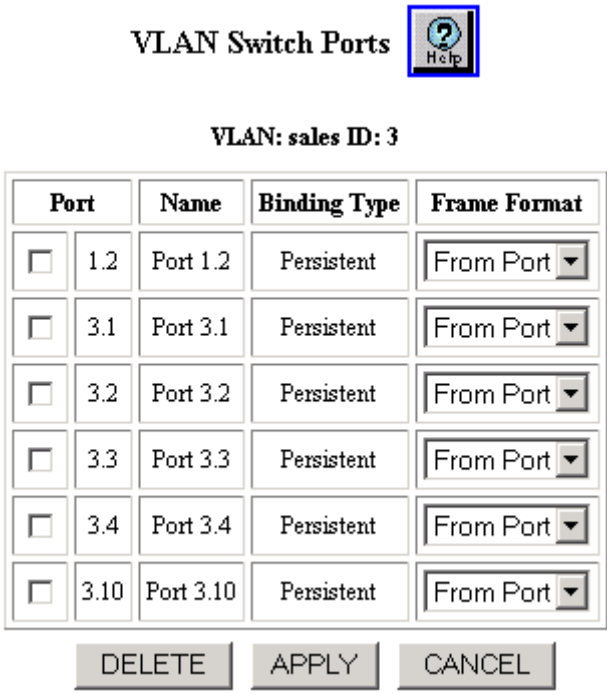
# Configuring VLAN Parameters

To configure all ports assigned to a VLAN:

1. Select **Configuration** from the **L2 Switching > VLANs** folder on the Web Agent window. The **VLAN Configuration** dialog box opens (Figure 4-3).

2. Click on the Name of the VLAN whose members you want to view. The **VLAN Switch Ports** dialog box opens (Figure 4-5).

***Figure 4-5. VLAN Switch Ports Dialog Box***



3. Refer to Table 4-2 to configure the **VLAN Switch Ports** dialog box parameters:

*Table 4-2. VLAN Switch Port Dialog Box Parameters*

| Parameter | Defines... |
|---|---|
| **Port** | The switch port associated with the VLAN. |
| **Name** | The switch default port name or the user assigned port name. |
| **Binding Type** | The binding types are set through the switch ports. Refer to the "Assigning VLANs to a Port and Associated Issues" section in Chapter 5.<br>• **Static** - when switch ports are added manually and can be removed<br>• **Persistent** - when switch ports are bound to VLANs automatically but can not be removed. automatically (i.e., if the binding for a switch port is set to 'Bind to All').<br>• **Dynamic** - when a switch port is assigned to VLAN using automatic VLAN binding,(i.e. if the binding for a switch port is set to “Bind to Received”). The VLAN may be deleted, but if the port VLAN binding is “Bind to Received”, the VLAN may be re-added by receiving tagged traffic. This causes the port to again dynamically bind to the VLAN.<br>Refer to “Configuring Port VLAN Parameters,” in Chapter 4 for more information. |
| **Frame Format** | • **From Port** - causes port to send frames using the frame format specified in the Trunk Mode attribute of the corresponding switch port.<br>• **Clear** - causes port to send untagged frames on this port for this VLAN.<br>**Note:** Refer to “Configuring Port VLAN Parameters,” in Chapter 4 for more information. |

4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Assigning Ports to VLANs

Refer to "Configuring Switch Port Parameters," in Chapter 5 for instructions on assigning ports to VLANs.

**CAUTION**

Before changing the VLAN that a port is assigned to, you must remove the port from the hunt group that the port is assigned to. Do *not* attempt to change the VLAN and remove the port from the hunt group simultaneously. If you do, the switch assigns all ports in the hunt group to the new VLAN.

# Spanning Tree Protocol Setup and Monitoring

The following information is provided in this section:

- Spanning Tree Protocol Implementation
- Managing the Spanning Tree Protocol
- Configuring Spanning Tree Protocol Ports

## Spanning Tree Protocol Implementation

This section introduces Spanning Tree Protocol, explains how it operates, and provides configuration procedures.

### What is Spanning Tree Protocol

The Spanning Tree Protocol is a layer 2 or bridging protocol that provides path redundancy while preventing undesirable loops in the bridged network. The Spanning Tree Protocol algorithm creates a single path through the network by ensuring that if more than one path exists between two parts of a network, only one of these paths is used, while the others are blocked.

*** Note:** The Spanning Tree Protocol (STP) Port Priority range has been changed. The values are now 1 to 15. If you changed the default range in an earlier release, you should verify that the priority is within the allowed range.

For more detailed information about the Spanning Tree Protocol, refer to the IEEE 802.1D standard for Media Access Control (MAC) bridges.

## Need for Spanning tree Protocol

For a bridging network to function properly, only one active path can exist between two stations. Multiple active paths between stations cause loops in the network. If a loop exists in the bridged network topology, the potential exists for message duplication, and in some cases a “Broadcast Storm”.

Spanning Tree Protocol defines a single spanning tree that spans all switches in a bridged network. It forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning Tree Protocol becomes unreachable, or if Spanning Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the bridge port by activating the standby path.

## Supported Spanning Tree Configurations

The Avaya Multiservice Switch supports four different Spanning Tree configurations.

- IEEE 802.1D
- Dual-Layer
- Per-VLAN (Default setting)
- Disabled

**IEEE 802.1D** - If you use the 802.1D spanning tree option all VLANs participate in the same spanning tree. The implication is that after resolving the spanning tree topology, a port will be forwarding, or blocked for all VLANs.

**Dual-Layer** - This option is to be used on a switch that is in between a 802.1D spanning tree domain switch and a per-VLAN domain switch. This option, allows the switch to terminate a legacy spanning tree (802.1D) from old bridges that are VLAN incapable, and interoperate with other per-VLAN spanning tree bridges.

**Per-VLAN** - If you use the Spanning Tree per VLAN option, each VLAN runs a separate spanning tree with its own BPDUs. This allows different ports to blocked or forwarding for different VLANs.

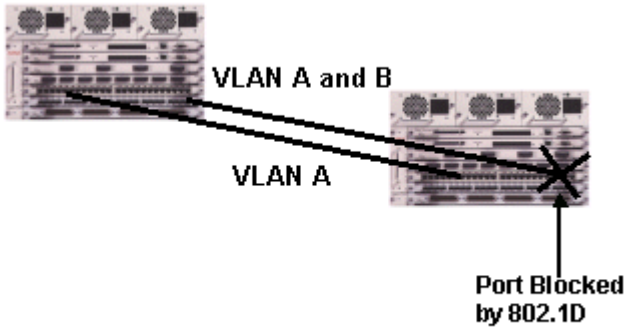
**Disabled** - Disables Spanning Tree for the entire switch.

### Problems with Single Spanning Tree Instance IEEE 802.1D

**Loss of Connectivity** - There is a the potential for the loss of connectivity of a VLAN when using standard Spanning Tree (IEEE 802.1D). Specifically when their is a loop in one VLAN, but not another, that share the same physical ports. In Figure 4-8, there is a loop in the physical connections between the two switches. This loop is in VLAN A, but not in VLAN B. When running single Spanning Tree, it is possible that in order to break the loop in VLAN A that a port that is blocked causes a loss of connectivity in VLAN B. Running per-VLAN Spanning Tree would correct the problem.

*** Note:** 802.1D configurations are typically used when only one VLAN is configured.

*Figure 4-6. Problems with 802.1D Spanning Tree*




## Managing the Spanning Tree Protocol

*** Note:** You should have a good understanding of the Spanning Tree Protocol before attempting to setup management parameters. Because of the number of “bridges” present in a switched networking environment, Spanning Tree Protocol structures can become extremely complex. For more information, refer to "Spanning Tree Modes" in Chapter 1.

You can manage the Spanning Tree Protocol using either the Web Agent or the CLI.

## Managing Spanning Tree Using the Web Agent

To manage Spanning Tree Protocol using the Web Agent:

1. Select **Spanning Tree** from the **L2 Switching** folder on the Web Agent window. The **Spanning Tree Information** window opens (Figure 4-7).

***Figure 4-7. Spanning Tree Information Dialog Box***

**Bridge Information**

| Bridge | Status | Bridge ID | Bridge Ports | Designated Root | Root Port | Root Cost | Top. Changes | Time Since Top. Change (hh:mm:ss) |
|---|---|---|---|---|---|---|---|---|
| Default | Enable | 0x800002E03B005C00 | 30 | 0x800002E03B005C00 | - | 0 | 1 | 01:04:17 |
| *autoVlan2 | Enable | 0x800002E03B005C00 | 2 | 0x800002E03B005C00 | - | 0 | 1 | 01:03:47 |
| *autoVlan3 | Enable | 0x800002E03B005C00 | 3 | 0x800002E03B005C00 | - | 0 | 1 | 01:04:07 |
| *autoVlan4 | Enable | 0x800002E03B005C00 | 2 | 0x800002E03B005C00 | - | 0 | 1 | 01:03:48 |
| *autoVlan155 | Enable | 0x800002E03B005C00 | 2 | 0x800002E03B005C00 | - | 0 | 1 | 01:03:41 |
| *autoVlan156 | Enable | 0x800002E03B005C00 | 2 | 0x800002E03B005C00 | - | 0 | 1 | 01:03:41 |
| *autoVlan157 | Enable | 0x800002E03B005C00 | 2 | 0x800002E03B005C00 | - | 0 | 1 | 01:03:43 |

2. Select the type of spanning tree you want to implement from the Configuration field pull-down menu.

Refer to Table 4-3 for a definition of the Configuration field parameters:

***Table 4-3. Spanning Tree Information Configuration Field Options***

| Parameter | Definition |
|---|---|
| **IEEE 802.1D** | Single IEEE 802.1D-compliant spanning tree for the entire bridge.<br>In 802.1D spanning tree mode, there is one root Bridge for the whole network, regardless of whether the switches support VLANs or not. Only one active data path is supported for all VLANs from any point in the network to any other point<br>**Note:** When the spanning tree mode is set to IEEE 802.1D, Bridge Protocol Data Units (BPDUs) are sent out ports in Clear (non-tagged) format even if the port has a tagged format (3Com, IEEE 802.1Q or Cisco ISL) defined. |
| **Per VLAN** | (Default Switch Setting) Each VLAN runs a separate IEEE 802.1D-compliant spanning tree.<br>In Per-VLAN spanning tree, the switch implements a separate spanning tree Domain for each VLAN. Each logical spanning tree has its own Per-VLAN BPDU's which are tagged with the appropriate VLAN identifier(s).BPDU's are sent clear (untagged) on clear trunks or tagged on tagged trunks. With Per-VLAN spanning tree a switch can participate in as many Spanning Tree Domains as there are VLANs defined on the switch.This allows for better use of links. Some may be blocked for one VLAN STP and forwarding traffic for another. |
| **Dual Layer** | Dual-Layer spanning tree is a variation of per-VLAN spanning tree. However, instead of using normal BPDUs which are clear (free of VLAN tags) on clear trunks and tagged on tagged trunks, as is the case with Per-VLAN Spanning Tree. Dual-layer uses a proprietary BPDUs. These proprietary BPDUs are sent to a special multicast address and contain information about which VLAN the BPDU is associated with.In the Dual-Layer Spanning Tree model, the switch terminates all 802.1D Spanning Tree Domains. The switch does not forward 802.1D BPDUs or participate in any 802.1D Spanning Tree Domains. It only participates in Spanning Tree Domains using a proprietary BPDU, which contains a VLAN identifier (VLAN ID). This proprietary Spanning Tree Protocol will resolve any loops in the switch. Legacy Bridges remain in separate Spanning Tree domains yet Loops between the Dual Layer Domains and Legacy domains cannot form. The Dual-Layer Spanning Tree method is preferred when inter-operating with large legacy bridge networks. Convergence time is reduced, and management is simplified, by allowing the legacy bridges to remain in their own spanning tree domain. |
| **Disable** | Global disable Spanning Tree for the entire switch.<br>*** Note:** Spanning tree can also be disabled on an individual port.Refer to the section labeled *Disabling Spanning Tree mode for this port* later in this chapter. |
| **Bridge** | Indicates a Bridge instance, in the figure a STP bridge per-VLAN |

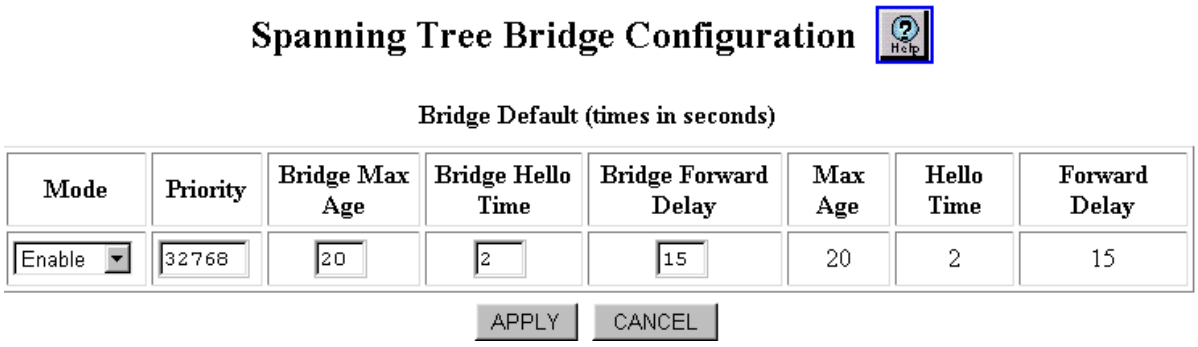
*Table 4-3. Spanning Tree Information Configuration Field Options*

| Parameter | Definition |
|---|---|
| **Status** | Indicates whether a bridge is enabled or disabled |
| **Bridge ID** | This bridge's ID |
| **Bridge Ports** | The number of ports in this bridge |
| **Designated Root** | Displays the Root bridge for this spanning tree |
| **Root Port** | Bridge port used to access the root bridge |
| **Root Cost** | Path cost to the root bridge |
| **Topology Changes** | Number of topology changes that have occurred since the last system reset |
| **Time Since Topology Change (hh:mm:ss)** | Number of hours, minutes, and seconds since the last topology change |

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

4. Select a VLAN name from the Bridge column (Figure 4-9)to set the bridge parameters. The Spanning Tree Bridge Configuration dialog box opens (Figure 4-10).

*Figure 4-8. Spanning Tree Bridge Configuration Dialog Box*



5. Refer to Table 4-4 to configure the Spanning Tree Bridge Configuration parameters:

***Table 4-4. Spanning Tree Bridge Configuration Parameters***

| Parameter | Definition |
|---|---|
| **Mode** | Determines whether spanning tree is enabled or disabled for this bridge.Default is Enabled |
| **Priority** | Spanning Tree Protocol Priority level for this bridge.<br>The Default value is 32768, the parameter range is 0-65535 |
| **Bridge Max Age (seconds)** | Sets the maximum amount of time that this bridge retains bridging information before discarding. When the maximum age expires, the bridge assumes it has lost connection to the network, and sends out requests to be re-added to the spanning tree.<br>The Default value is 20 sec., the parameter range is 6-40 sec. |
| **Bridge Hello Time (seconds)** | Time between generation of BPDUs by the root bridge.The Default value is 2 sec., the parameter range is 1-10 sec. |
| **Bridge Forward Delay (seconds)** | Amount of delay used when a port transitions to the forwarding state. Set by the root bridge for the segment. The Default value is 15 sec., the parameter range is 4-30 sec. |
| **Max Age (seconds)** | Current maximum age for this spanning tree. Determined by the root bridge. |
| **Hello Time (seconds)** | Current hello time for this spanning tree. Determined by the root bridge. |
| **Forward Delay (seconds)** | Current forwarding delay for this spanning tree. Set by the root bridge. |

*** Note:** The Avaya Multiservice switch enforces the following spanning tree parameter relationships, as defined by IEEE 802.1D.

- 2X (Bridge_Forward-delay-1.0 seconds)>= Bridge_Max_Age
- Bridge_Max_age>= 2x (Bridge_Hello_Time + 1.0 seconds)

6. Click APPLY to save your changes, or CANCEL to restore previous settings.

### Using the CLI

To manage spanning trees using the CLI, enter the following command from Configure mode:

```
(configure)# set spantree
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Configuring Spanning Tree Protocol Ports

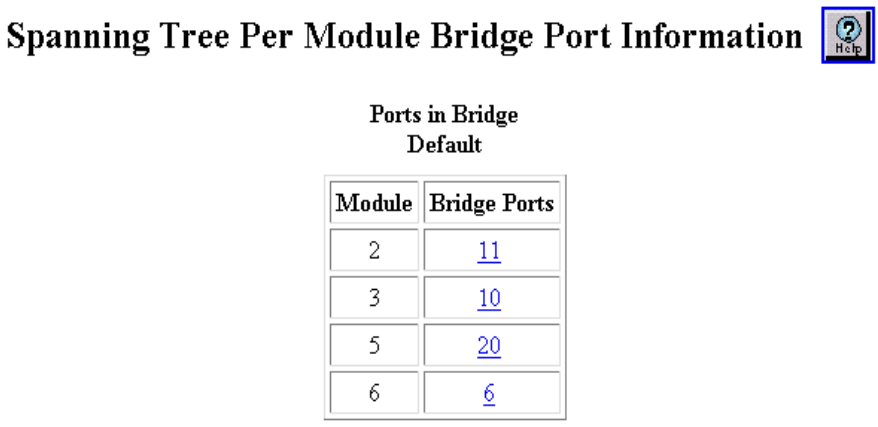
You can configure the bridge ports for Spanning Tree using either the Web Agent or the CLI.

### Using the Web Agent

To configure spanning tree bridge ports using the Web Agent:

1. Select **Spanning Tree** from the **L2 Switching** folder on the Web Agent window. The **Spanning Tree Information** window opens (Figure 4-9).
2. Select the port number listed in the **Bridge Ports** column. The **Spanning Tree Per Module Bridge Port Information** window opens (Figure 4-11).

***Figure 4-9. Spanning Tree Per Module Bridge Port Dialog Box***



3. Select the **Bridge Port** number from the **Bridge Ports** column. The **Spanning Tree Bridge Port Information** window opens (Figure 4-12).

*Figure 4-10. Spanning Tree Bridge Port Information Window*

**Spanning Tree Bridge Port Information**

Ports in Bridge Default, Module 7

| Bridge Port | Port | Name | State | Designated Root | Designated Bridge | Des. Port | Des. Cost | Fwd. Trans. |
|---|---|---|---|---|---|---|---|---|
| 265 | 7.1 | Port 7.1 | Fwding | 0x800000306D605C00 | 0x800000306D605C00 | 0x8109 | 0 | 1 |
| 266 | 7.2 | Port 7.2 | Fwding | 0x800000306D605C00 | 0x800000306D605C00 | 0x810A | 0 | 1 |
| 267 | 7.3 | Port 7.3 | Down | - | - | - | - | 0 |
| 268 | 7.4 | Port 7.4 | Down | - | - | - | - | 0 |
| 269 | 7.5 | Port 7.5 | Down | - | - | - | - | 0 |
| 270 | 7.6 | Port 7.6 | Down | - | - | - | - | 0 |

Table 4-5 explains the **Spanning Tree Bridge Port Information** window parameters.

*Table 4-5. Spanning Tree Bridge Port Information Window Parameters*

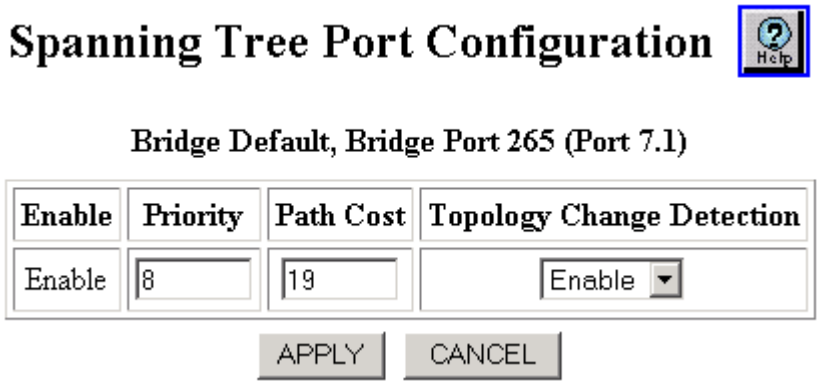
| Parameter | Explanation |
|---|---|
| **Bridge Port** | The bridge port. |
| **Port** | The spanning tree bridge port number. |
| **Name** | The name assigned to the bridge port. |
| | ***1 of 2*** |

*Table 4-5. Spanning Tree Bridge Port Information Window*

| Parameter | Explanation |
|---|---|
| **State** | Current bridging state of the port.<br>The options are:<br>• **Disabled** - The port is disabled.<br>• **Blocking** - The Spanning Tree algorithm has set this port's state to block, meaning that it is enabled, but not passing traffic.<br>• **Listening** - The port is in a transitional state, listening for BPDUs and waiting for the spanning tree algorithm to determine if the port should transition to the Learning state. The port is still in blocking mode.<br>• **Learning** - The port is learning new MAC addresses, but not yet forwarding traffic.<br>• **Forwarding** - This port has been selected by the Spanning Tree algorithm to forward traffic, and is forwarding traffic currently.<br>• **Down** - The port's physical port has no link detected. |
| **Designated Root** | Displays the Root bridge for this spanning tree. |
| **Designated Bridge** | The bridge identifier for the bridge considered to be the designated bridge for this segment. |
| **Designated Port** | The port identifier of the port on the designated bridge for this segment of the spanning tree. |
| **Designated Cost** | The path cost of the designated root of the segment connected to this port. |
| **Forward Transitions** | Number of times that this port has transitioned from blocking to forwarding. |
| | *2 of 2* |

4. In the **Bridge Port** column, select the bridge port number The **Spanning Tree Port Information** window opens (Figure 4-13).

*Figure 4-11. Spanning Tree Port Configuration Window*




5. Enter the appropriate information for the parameters. For an explanation of the parameters in the Spanning Tree Port Configuration dialog box, refer to Table 4-6

*Table 4-6. Spanning Tree Port Configuration Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Enable** | Indicates whether or not spanning tree is active on this bridge port. |
| **Priority** | Sets the port's priority in the spanning tree algorithm. A port with a higher priority (lower priority number) is more likely to be chosen as the primary path in the spanning tree. The Default setting is 8. The parameter range is from 0-15 |
| **Path Cost** | Sets the spanning tree path cost for this port. The ports that you prefer be used by the spanning tree should have the lowest path cost. The Default setting is based on port link speed. The parameter range is 1-65535 |
| **Top. Change Detection** | Allows you to enable or disable topology change detection. Specifies whether a Topology Change Notification (TCN) packet is sent through the root port (or if this switch is the root bridge, whether or not Fast Aging occurs) whenever the port enters the forwarding or blocking states. This attribute should be enabled on ports which connect to other switches. The default value is enabled. |
| | |

6. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Using the CLI

To configure spanning tree bridge ports using the CLI, enter the following command from Configure mode:

```
<config># set port spanning-tree-mode {<mod-num> |
<mod-swport-range>}[...,{<mod-num> | <mod-swport-
range>}]{disable | enable}
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Disabling Spanning Tree Mode for the Port

You can disable Spanning Tree mode for the port from either the Web Agent or the CLI.

*** Notes:** When disabling the Spanning Tree Protocol for a port, BPDUs received on that port are ignored and are not generated. The port moves directly into the forwarding state from the disabled state and does not trigger a topology detection change.

It is recommended that you set Spanning Tree to per-VLAN for IEEE 802.1Q or Multi-Layer trunking modes, trunked ports. This prevents an entire link from being blocked when there is a loop in one VLAN.

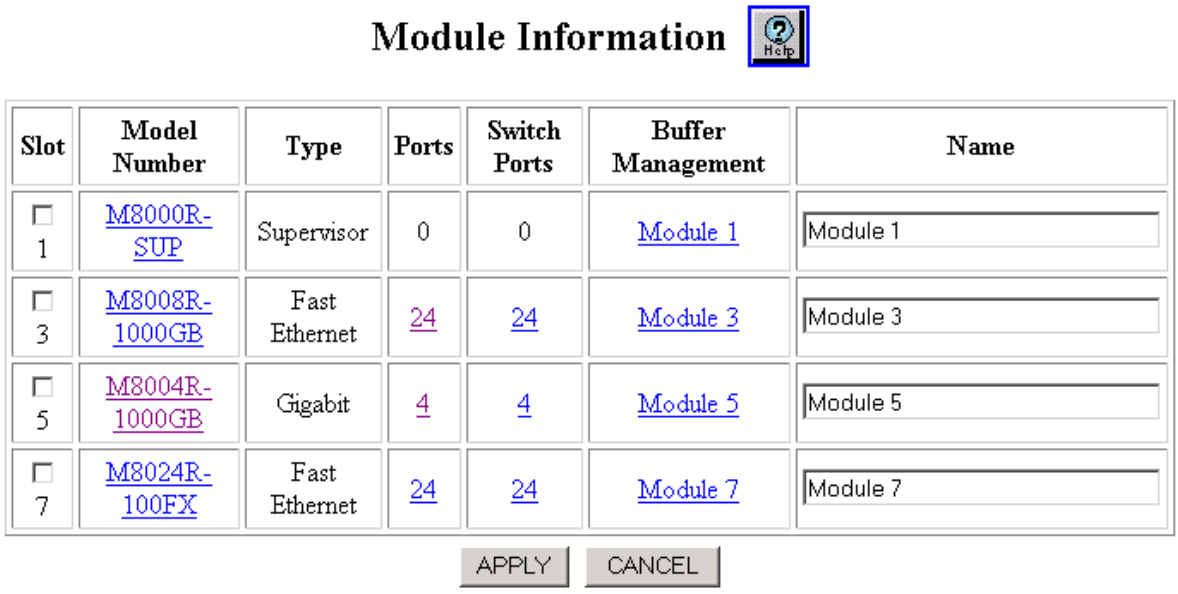
If you have an ATM Uplink module installed, and there is a loop through the uplink, the ATM Uplink module does not function properly if you use IEEE802.1D.

## Using the Web Agent

To disable spanning tree mode for the port using the Web Agent:

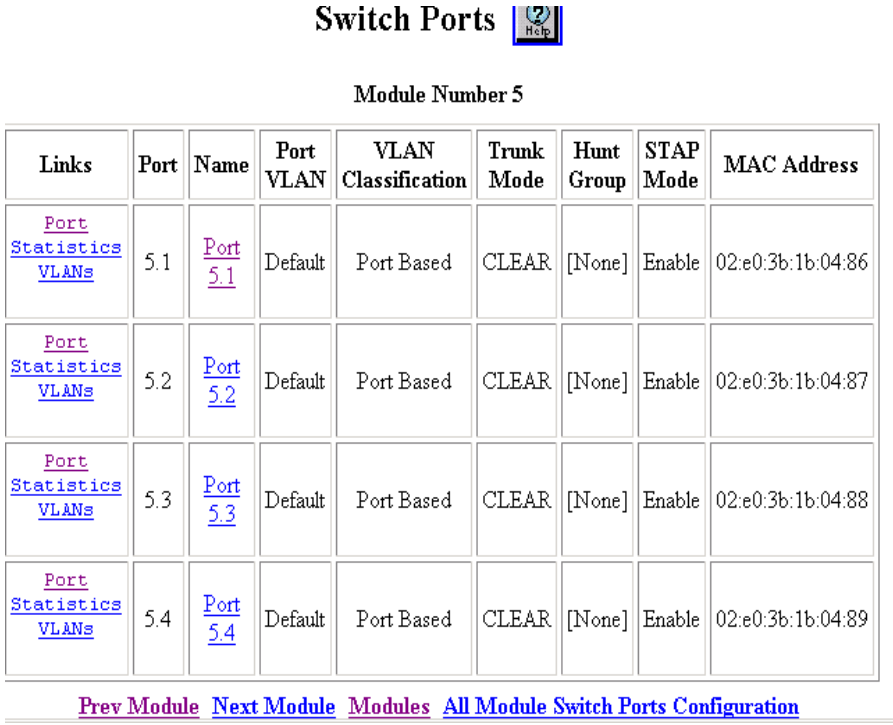
1. Select **Configuration** from the **Modules and Ports** window. The **Module Information** window opens (Figure 4-14).

*Figure 4-12. Module Information Window*




2. Select the switch port number from the **Switch Ports** column. The **Switch Ports** window opens (Figure 4-15).

*Figure 4-13. Switch Ports Dialog Box*



Switch Ports

Module Number 5

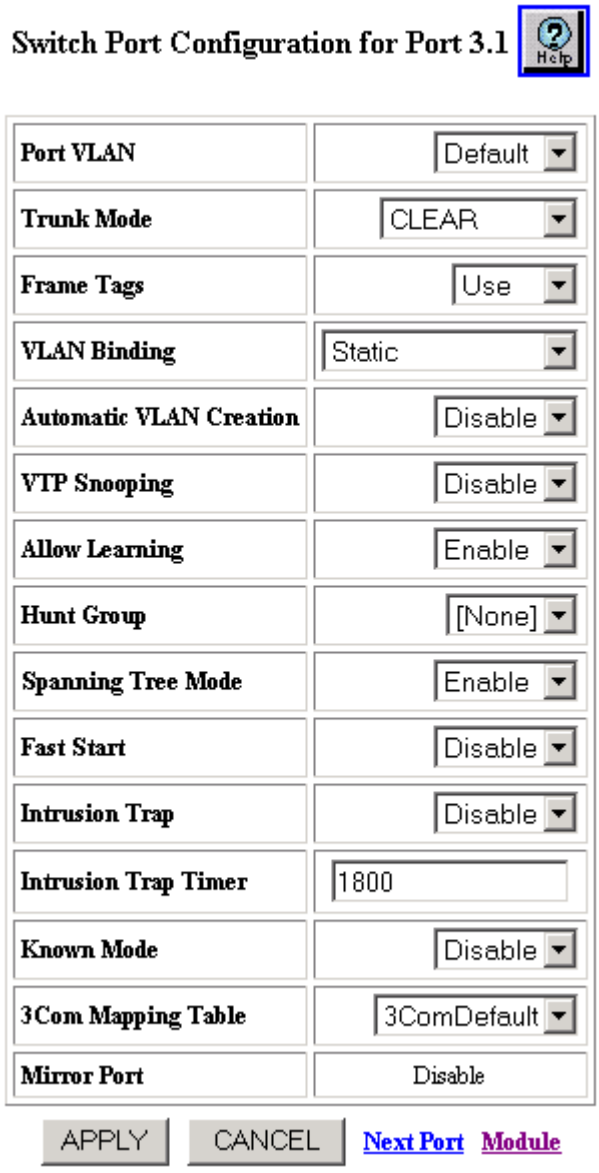
| Links | Port | Name | Port VLAN | VLAN Classification | Trunk Mode | Hunt Group | STAP Mode | MAC Address |
|---|---|---|---|---|---|---|---|---|
| Port Statistics VLANs | 5.1 | Port 5.1 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:86 |
| Port Statistics VLANs | 5.2 | Port 5.2 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:87 |
| Port Statistics VLANs | 5.3 | Port 5.3 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:88 |
| Port Statistics VLANs | 5.4 | Port 5.4 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:89 |

Prev Module Next Module Modules All Module Switch Ports Configuration

3. Select the port number on which you want to disable spanning tree from the **Name** column.

   The **Switch Port Configuration** window for that port opens (Figure 4-16).

*Figure 4-14. Switch Port Configuration Window*




4. From the Spanning Tree pull-down menu, for the **Spanning Tree Mode** parameter select **Disable**.

5. Click **Apply** to disable spanning tree mode on the port, or **CANCEL** to keep spanning tree mode enabled on the port.

### Using the CLI

To Disable Spanning Tree mode on a port using the CLI, enter the following command from Configure mode:

```
<configure># set port spanning-tree-mode <mod-num>
or <mod-swport-range> disable
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

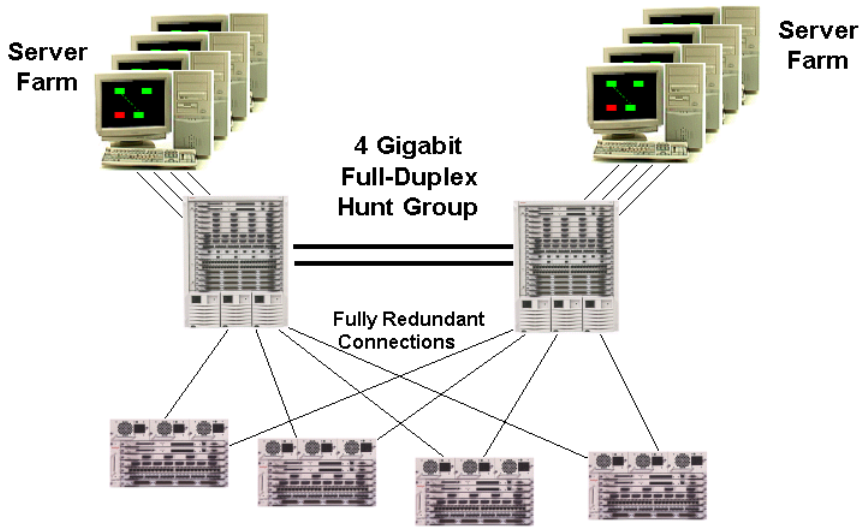
# Using Hunt Groups to Aggregate Bandwidth between Switches

### Hunt Group Overview

Hunt groups allow you to aggregate multiple switch ports to act as one switch port, effectively combining the bandwidth into a single connection. Frames sent to the Hunt Group will be transmitted by one of the ports in the Hunt Group. Hunt Groups load share traffic across all member ports, this aggregates the bandwidth of the Hunt Group ports. Hunt groups also provide fault tolerance. If a port in a hunt group fails, the remaining ports in the hunt group will assume the traffic and continue forwarding.

***Figure 4-15. Hunt Group Example***

### Hunt Group example



Hunt Groups expand the capacity of the core switched backbone. While there is no specific limit on the number of ports in a Hunt Group (see the section labeled Hunt Group configuration considerations). In the example, (Figure 4-17), the Hunt Group consists of two full-duplex Gigabit Ethernet links shared between two switches, for an aggregate capacity of 4 Gbps. Enterprise-level servers can be directly attached to the switching core using either 100 Mbps or Gigabit Ethernet connections. Fault-tolerant spanning tree links from the core to the next level of network spread the distribution and capacity to building or departmental switching centers. Each of these next-level switches may in turn support tens (or even hundreds) of workgroup switches and users.

### Features

Hunt group features include:

- Shared traffic load.
- Fault tolerance — If a port in a group fails, the remaining ports in the group pick up the traffic load.
- Support for any number of same-speed same media type connections in a group — The group is not restricted to a single module in a switch.
- Quicker recovery from link failure — If a port in the group fails, the remaining ports carry the load. Recovery is not limited by Spanning Tree Protocol convergence time (convergence time is the time the network takes to resume steady-state forwarding after Spanning Tree Protocol reconfiguration).
- Supports up to 25 hunt groups per switch, if 48-port mode is disabled and up to 13 hunt groups if 48-port mode is enabled.

## Hunt Group Terminology

**Base Port/Flood port**- When the hunt group is configured, there is one port designated “Base Port”. All ports in the hunt group assume the identity of the base port. The base port passes all flood frames, broadcast frames, destination unknown unicast, and multicast frames for VLANs associated with the hunt group. Spanning Tree treats all ports in the hunt group as one port. The base port sends and receives Bridge Protocol Data Units (BPDU’s).

**Member port** - A port that is a member of the hunt group. Sometimes referred to as a “Participating port”.

**Non-member port** - A port that is not a member of a hunt group. sometimes referred to as a “non-Participating port”.

**Forwarding Engine (FE)** - A generic name for hardware that makes layer 2 and layer 3 forwarding decisions.

**Participating (or Non-Participating) Forwarding Engine** - A forwarding engine that has a port is part of the Hunt Group. Example, a M8024 (80 series module with 24 10/100 Mbps ports), the first 12 ports are serviced by a single Forwarding Engine. If any of those 12 ports participates in a hunt group, then that Forwarding Engine is considered a participating forwarding engine.

# How Hunt Groups Load Share

## Forwarding Engines and Fabric Ports

Each 80 series Media module has at least two Forwarding Engines, and as many as eight. These engines are the major hardware components for bridging and routing data traffic. The Forwarding Engines can service up to twelve 10/100 Mbps ports. Example, 24-port 10/100 Mbps 80 series media module has two Forwarding Engines that service twelve 10/100 Mbps ports each. An eight-port Gigabit module has eight forwarding engines one for each of the Gigabit ports per slot. Refer to Table 4-7 for the relationship of media modules (50 and 80 series) to Forwarding Engines.

## 80 Series Forwarding Engines

The Forwarding Engines are numbered starting at one and increased by one for each Forwarding Engine. The Supervisor module always has Forwarding Engines numbered one and two. For a 7-slot P580 switch, numbers one and two for the Supervisor module and up to eight per media module slot for a maximum total of 50 Forwarding Engines. For a 17-slot P882, numbers one and two for the Supervisor module and up to eight for each of the media modules, for a maximum total of 130. The numbering sequence will vary depending on the type and total number of media modules. If the switch has empty slots the numbering sequence is bypassed for the empty slots.

## Fabric Ports

The P580/P882 has two backplane connections or ports for each media module. These ports connect the media modules to the backplane Cross Bar Switch Fabric, which in turn connects all modules to all other modules and ports. These ports are referred to as “Switch Fabric Ports”. There are two Switch Fabric ports per media module slot (slots 2 through 7, or slots 2-17) and one fabric port for the Supervisor slot (slot 1) (Figure 4-18).Each 80 series media module can use up to two fabric ports in the slot, the number of Forwarding Engines to fabric ports varies with the media module.There is anywhere from one to four Forwarding Engines per fabric port for each 80 series media module (Table 4-7).

The number of Forwarding Engines are distributed among the ports for 80 series modules. The 80 series 10/100 Mbps media modules are distributed with 12 10/100 ports for each Forwarding engine. For example, the 48 port 10/100 media module has four Forwarding Engines. The first 12 (1-12) ports are on the first Forwarding Engine, the second 12 (13-24) are on the second Forwarding Engine, which in turn use one fabric port, the third and fourth grouping of 12 ports each have a Forwarding Engine and use the second fabric port. The Forwarding Engines are distributed on a one to one basis for the 80 series Gigabit media modules. For example the 8 port 1000 TX, the first four ports have four Forwarding Engines, one for each Gigabit port (1-4), and uses one fabric port, the other four ports (5-8) also have four Forwarding Engines, which use the second fabric port.

## 50 Series Forwarding Engines and Fabric Ports

On a 50 series layer 3 module, each fabric port has two Forwarding Engines, one for layer 3 traffic, and one for layer 2 traffic. All layer 3 traffic will be associated with one Forwarding Engine and all the layer 2 traffic will be associated with the other Forwarding Engine.

Example, the twelve-port 10/100 layer 3 50 series media module, layer 3 traffic is coming in the first port and the last port, (ports 1,12). Using the 80 series even distribution, the first six ports are associated with one FE and the second six ports with the second FE, and distributed across both fabric ports.

This is different for the 50 series modules. The twelve port layer 3 50 series media module, all twelve ports are associated with one Forwarding Engine for layer 3 traffic and one Forwarding Engine for layer 2 traffic. In addition only one fabric port is used for all twelve ports.

## Load Share Function

Hunt Groups load share by directing different traffic to different ports in the hunt group, when sending traffic to a particular user. Load sharing is done in a round-robin fashion across the ports in a hunt group. This is based upon **BOTH** the **Destination MAC Address** and the **Source Forwarding Engine**. The Hunt Group ports on which unicast packets traverse to reach the destination depends upon the source user's associated Forwarding Engine.

## Hunt Group Example

Refer to Figure 4-17. One port in the Hunt Group will be designated as the "Base"/"Flood Port". All flood traffic for all VLANs is sent through this port only. All ports are members of all VLANs associated with the Hunt Group Base port. There are 8 non-member Forwarding Engines. Load sharing is accomplished by using the combination of the Source Forwarding engine and the Destination MAC Address to assign a hunt group port. Users A and B are associated with FE#9 and therefore the first port in the Hunt group will be used for unicast packets from A to Destination E and from B to E. Users C and D are associated with FE#10 and therefore the second port in the Hunt Group will be used for unicast packets from C to E and D to E.

When MAC Address E is learned, it is assigned to the first hunt group port for FE#1, the second hunt group port for FE#2, the first port for FE#3, the second port for FE#5, the first port for FE#7, the second port for FE#8, the first for FE#9, and the second port for FE#10. The second destination MAC Address is round-robin assigned in the same fashion and so on.

***Figure 4-16. Slot to Fabric Port relationship***

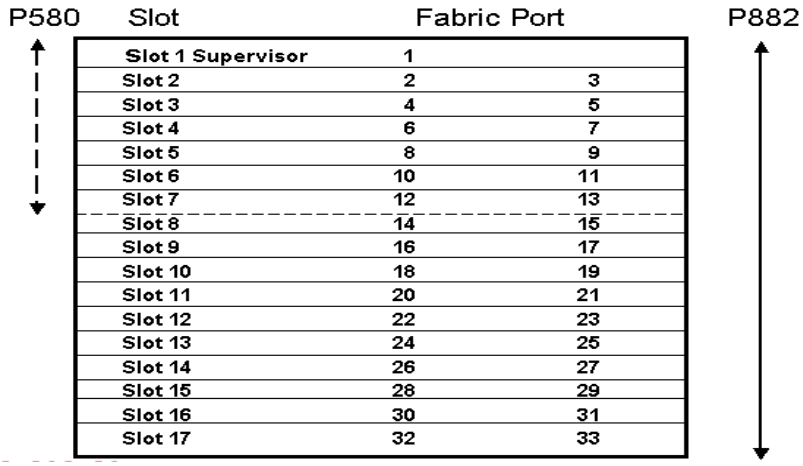
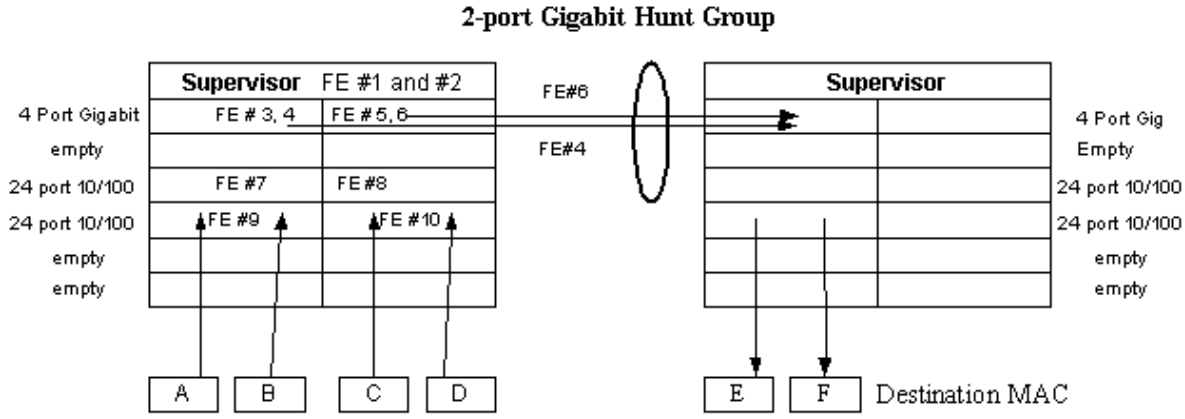


*Table 4-7. Module Forwarding Engines and Fabric Ports*

| Module Type | Total Number of forwarding engines | Number of Fabric Ports | Description |
|---|---|---|---|
| 80 series M8000R Supervisor | 2 | 1 | FORE port, CPU |
| 80 series 24 port 10/ 100Mbps TX and 100Mbps FX | 2 | 2 | 1 forwarding engine per fabric port |
| 80 series 48 port 10/ 100Mbps | 4 | 2 | 2 forwarding engines per fabric port |
| 80 series 4 port Gigabit Fiber or TX | 4 | 2 | 2 forwarding engines per fabric port |
| 80 series 8 port Gigabit Fiber or TX | 8 | 2 | 4 forwarding engines per fabric port |
| 50 series M5500R Supervisor | 2 | 1 | FORE port, CPU |
| 50 series 10 port 100Mbps FX(layer 2) | 1 | 1 | 1 forwarding engine to 1 fabric port only |
| 50 series 10 port 100Mbps FX (layer 3) | 2 | 1 | 2 forwarding engines to 1 fabric port only |
| 50 series 12 port 10/ 100 TX (layer 3) | 2 | 1 | 2 forwarding engines to 1 fabric port |
| 50 series 2 port Gigabit Fiber (layer 2) | 2 | 2 | 1 forwarding engine to 1 fabric port |
| 50 series 2 port Gigabit Fiber (layer 3) | 4 | 2 | 1 forwarding engine to 1 fabric port |
| 50 series 4 port Gigabit Fiber (layer 2) | 4 | 2 | 2 forwarding engines per fabric port |
| 50 series 20 port 10/ 100Mbps TX (layer 2) | 2 | 2 | 1 forwarding engine per fabric port |

Note: All 80 series media modules are L3 capable

*Figure 4-17. Load Sharing Example*




## Optimizing Hunt Group Throughput

To Optimize Hunt Group throughput follow these considerations.

- Forwarding Engines in the Hunt group ports should be separate from the ports involved in the modules traffic flows.
- The greater the number of non-member Forwarding Engines in the system, the greater the ability of the system to load-share.
- Distribute the hunt group across more than one Fabric Port per slot
- Distribute the hunt group across media modules

# Hunt Group Configuration Considerations

Consider the following before creating hunt groups:

- Hunt group end to end physical connections must be configured with the hunt group ports connected to hunt group ports.
- All ports of the hunt group must be of the same bandwidth and all layer 2 or all layer 3 ports (but not a mix)
- Can have a mix of 80 and 50 series as long as they are the same bandwidth and all layer 2 or all layer 3. (but not a mix)
- A hunt group cannot be distributed between more than two switches.
- You must disable or disconnect the ports in a hunt group until both ends of the link are configured.
- All ports in the hunt group take on the configuration of the base port
- Both sides of the hunt group have the same configuration
- Any change to a port in the hunt group will be reflected on all ports.
- When removing a port from a hunt group with the Web Agent, it must be removed before its VLAN assignment is changed.
- If 48-port mode is enabled on the switch, only the *first thirteen hunt groups* are retained and all others are discarded. However, the ports associated with the discarded hunts groups lose their hunt group bindings, but still retain their VLAN bindings, and are still active as VLAN bridges. Spanning tree may or may not, due to the topology or spanning tree settings on those ports, decide to forward traffic over unwanted trunks.

# Creating Hunt Groups

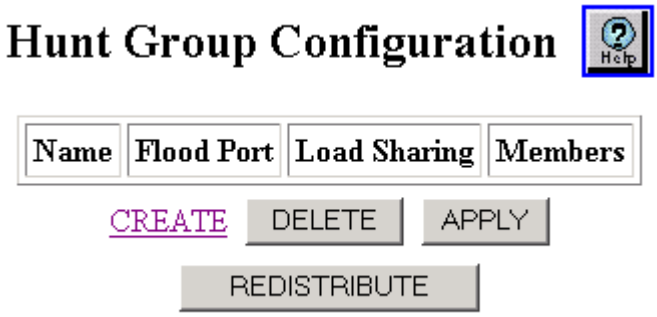
You can create hunt groups from either the Web Agent or the CLI.

## Using the Web Agent

To create a hunt group using the Web Agent:

1. Select **Hunt Groups** from the **L2 Switching** group in the Web Agent window. The Hunt Group configuration window opens. Figure 4-18.

*Figure 4-18. Hunt Group Configuration Window*




2. Select **CREATE**. The **Create Hunt Group** dialog box opens (Figure 4-19).

*Figure 4-19. Create Hunt Group Dialog Box*

3. Enter a name for the hunt group in the **Name** field. A Unique Name assigned to the Hunt Group. A maximum of 31 alphanumeric characters.

4. Select **Enable** from the **Load Sharing** pull-down menu to enable **Load Sharing** for the Hunt Group.

5. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

# Adding Ports to the Hunt Group

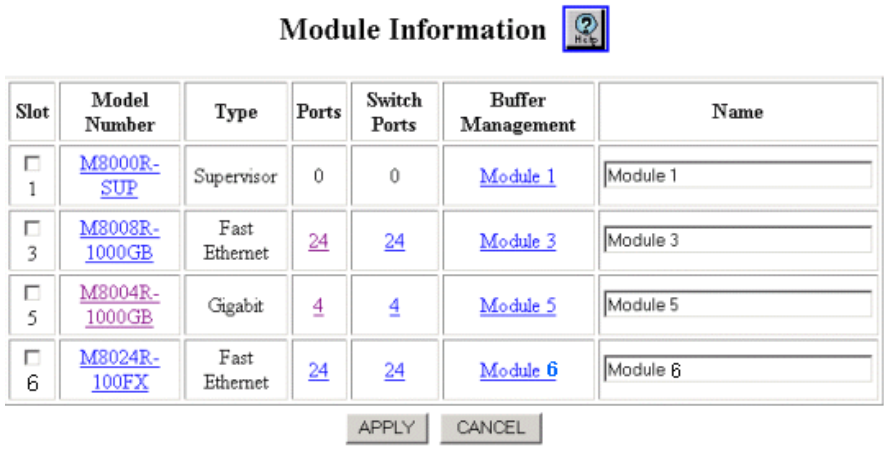
Once you have created and named a Hunt Group, you can add as many additional ports as needed to the Hunt Group. The next two Hunt Group configuration steps, adding physical ports, and switch ports to the Hunt Group, can be done using the Web Agent or the CLI.

## Using the Web Agent

To add ports to a hunt group using the Web Agent:

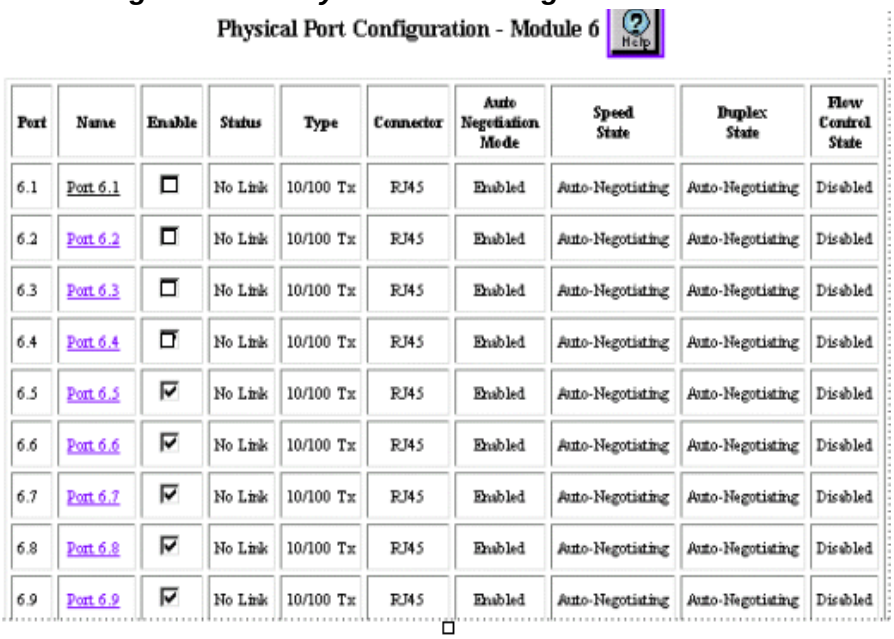
1. Select **Configuration** from the **Modules and Ports** folder on the Web Agent window. The **Module Information** window opens (Figure 4-20).

***Figure 4-20. Module Information Window***




2. Select a port number from the **Ports** column. The **Physical Port Configuration** window opens (Figure 4-21).

*Figure 4-21. Physical Port Configuration Window*




| Port | Name | Enable | Status | Type | Connector | Auto Negotiation Mode | Speed State | Duplex State | Flow Control State |
|---|---|---|---|---|---|---|---|---|---|
| 6.1 | Port 6.1 | ☐ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 6.2 | Port 6.2 | ☐ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 6.3 | Port 6.3 | ☐ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 6.4 | Port 6.4 | ☐ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 6.5 | Port 6.5 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 6.6 | Port 6.6 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 6.7 | Port 6.7 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 6.8 | Port 6.8 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 6.9 | Port 6.9 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |

3. Uncheck the checkbox from the **Enable** column for a specific port. The check mark disappears to disable the port.

*** Note:** Check the speed of the ports that you are configuring into the Hunt Group. The ports must be physically connected to each other (for example, in a four-port Gigabit hunt group, ensure that you have four fiber cables with switch ports connected at each end).Also Auto-negotiation should be disabled on the ports to further insure against speed mismatch

— If this is a new hunt group, disable all of the ports you are adding to the hunt group.

— If you are adding ports to an existing hunt group, disable the ports you are adding.

4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Adding Switch Ports to the Hunt Group

1. Select **Modules** at the bottom of the **Physical Port Configuration** dialog box. The Module Information dialog box re-opens.(Figure 4-20). As an alternate procedure, select Configuration > Modules and Ports > Module Information window.

2. Select a number from the **Switch Ports** column, for the module whose port(s) you are adding to the hunt group. The **Switch Ports** dialog box opens (Figure 4-22).

***Figure 4-22. Switch Ports Window***

**Switch Ports**

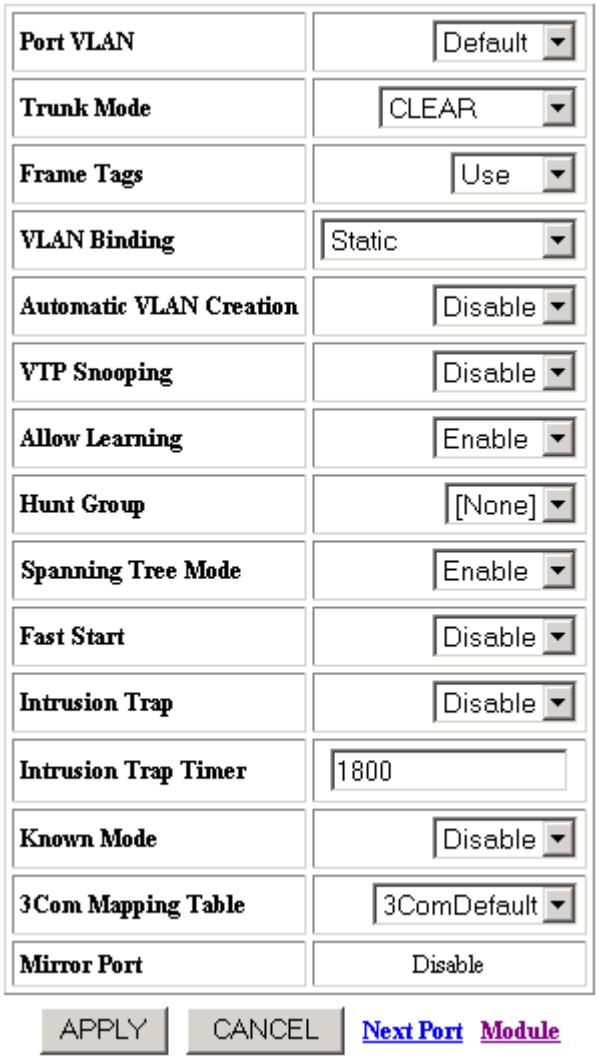
**Module Number 5**

| Links | Port | Name | Port VLAN | VLAN Classification | Trunk Mode | Hunt Group | STAP Mode | MAC Address |
|---|---|---|---|---|---|---|---|---|
| Port Statistics VLANs | 5.1 | Port 5.1 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:86 |
| Port Statistics VLANs | 5.2 | Port 5.2 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:87 |
| Port Statistics VLANs | 5.3 | Port 5.3 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:88 |
| Port Statistics VLANs | 5.4 | Port 5.4 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:89 |

Prev Module Next Module Modules All Module Switch Ports Configuration

3. Select the name of the port you want to configure from the **Name** column. The **Switch Port Configuration** window for that switch port opens (Figure 4-23).

*Figure 4-23. Switch Port Configuration Window*




4. Select the hunt group assignment from the **Hunt Group** pull-down menu.

5. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

6. Repeat Steps 1-9 for any additional ports that you want to add to this hunt group.

7. Repeat steps 1 through 10 on the switch at the other end of the hunt group connection.
8. Select **Configuration** from the **Modules & Ports** folder on the Web Agent window. The **Module Information** window re-opens (see Figure 4-20).
9. Select a port number from the **Ports** column. The **Physical Port Configuration** window opens (see Figure 4-21).
10. Select a checkbox from the **Enable** column for that port. The group can now function as a load-sharing connection.
11. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

*** Note:** If thousands of addresses have been learned on a port and a link in the hunt group goes down, the switch-over of traffic between ports may take several seconds.

*** Note:** If you use static VLAN binding and hunt groups, make sure to first bind all the VLANs to all the ports that you will use in the hunt group and then apply the hunt group to those ports.

## Creating Hunt Groups Using the CLI

To create a hunt group using the CLI, enter the following command from Configure mode:

```
<configure># set huntgroup <huntgroup-name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Viewing Hunt Group Members

You can view Hunt Group members from either the Web Agent or the CLI.

## Using the Web Agent

To view details about hunt group members using the Web Agent:

1. Select **Hunt Groups** from the **L2 Switching** folder in the Web Agent window. The **Hunt Group Configuration** window opens (Figure 4-24).
2. Select a underlined number in the **Members** column. The **Hunt Group Members** window opens with pertinent information about the members of that hunt group (Figure 4-24)

***Figure 4-24. Hunt Group Members Dialog Box.***

### Using the CLI

To view details about hunt group members using the CLI, enter the following command in configuration mode:

```
<configure># show huntgroup <huntgroup-name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

To add ports to a hunt group using the CLI, enter the following command from Configure mode:

```
<configure># set port huntgroup
{<mod-num>|<mod-swport-range>}
[...,{<mod-num>|<mod-swport-range>}]<huntgroup-
name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Removing Ports from Hunt Groups

You can remove a port from a hunt group by using either the Web Agent or the CLI.

### Using the Web Agent

To remove a port from a hunt group by using the Web Agent:

1. Open the **Switch Port Configuration** window for the port that you want to remove.
2. Click **None** in the **Hunt Group** field.
3. Click **Apply**.

### Using the CLI

To remove a port from a hunt group by using the CLI:

1. Enter Global Configuration mode.

   The CLI displays the `Avaya(configure)#` prompt.

2. Enter the following command:

   `<configure># clear port huntgroup` <mod-swport>

   where <*mod-swport*> is the slot number of a module and a port number. For example, to specify port 1 on the module in slot 3, enter **3/1**.

# Configuring VLAN Trunk Protocol (VTP) Snooping

Enabling VLAN Trunk Protocol (VTP®) Snooping on the Avaya Multiservice switch allows it to automatically synchronize its VLAN configuration with that of a Cisco VTP server switch. VTP is a Cisco® layer 2 protocol used to maintain VLAN configuration consistency among switches. Both switches must be on the same network, have at least VLAN 1 (Default) bound to a connecting link that is forwarding according to the Spanning Tree Protocol, and both ends of the link have the same Trunk Mode setting. Valid Trunk Mode options that work with VTP Snooping are Cisco Inter-Switch Link (Multi-layer) and IEEE 802.1Q.

VLAN additions, deletions, and name changes made on the network's Cisco VTP server are automatically updated on Avaya Multiservice switches that have VTP Snooping enabled and are connected to the Cisco VTP server with the same VTP Domain name. VLAN changes made on an Avaya Multiservice switch are not automatically updated on any other switch. Please note that VTP learned VLANs may not be modified or deleted on an Avaya Multiservice switch while VTP is enabled. This restriction is in place to help maintain VLAN configuration consistency among VTP Snooping switches within the VTP Domain. Also the Avaya Multiservice switch handles VLAN name or VLAN ID conflicts between itself and a VTP server by giving locally configured VLANs precedence. For example if a VLAN ID or VLAN name is received in a VTP message that is also configured locally on an Avaya Multiservice switch, the VTP message's VLAN information is ignored for that VLAN and a message is entered in the switch's event log indicating the condition.

*** Note:** VTP Snooping is **Disabled** by default. You only need to change VTP Snooping port settings if you want to Enable its ability to learn VLAN changes from a Cisco VTP server.

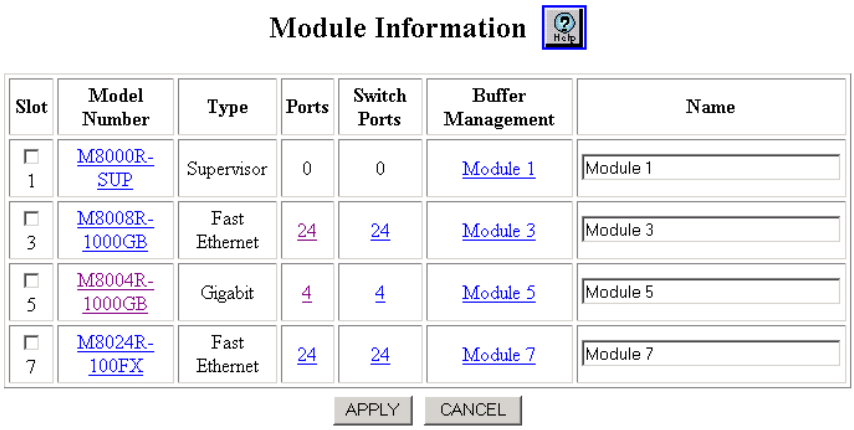
You can configure VTP snooping from either the Web Agent or the CLI.

## Using the Web Agent

To configure VTP snooping using the Web Agent:

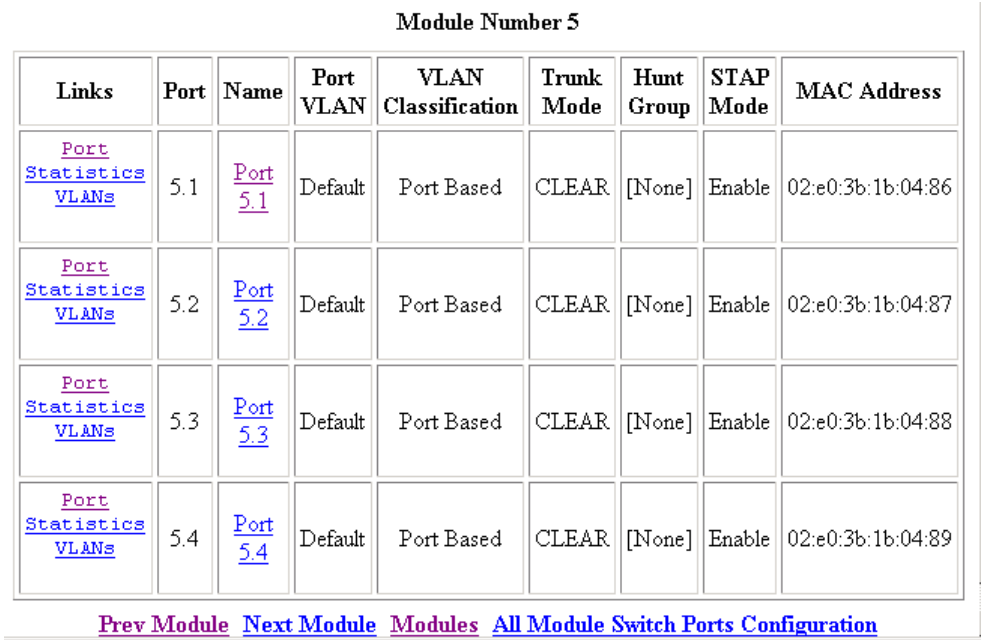
1. Select **Configuration** from the **Modules & Ports** folder on the Web Agent window. The **Module Information** window opens (see Figure 4-25).

***Figure 4-25. Module Information Window***



2. Select the number in the **Switch Ports** column for the module you want to configure VTP. The **Switch Ports** window for that module opens (see Figure 4-26).

*Figure 4-26. Switch Ports Window*



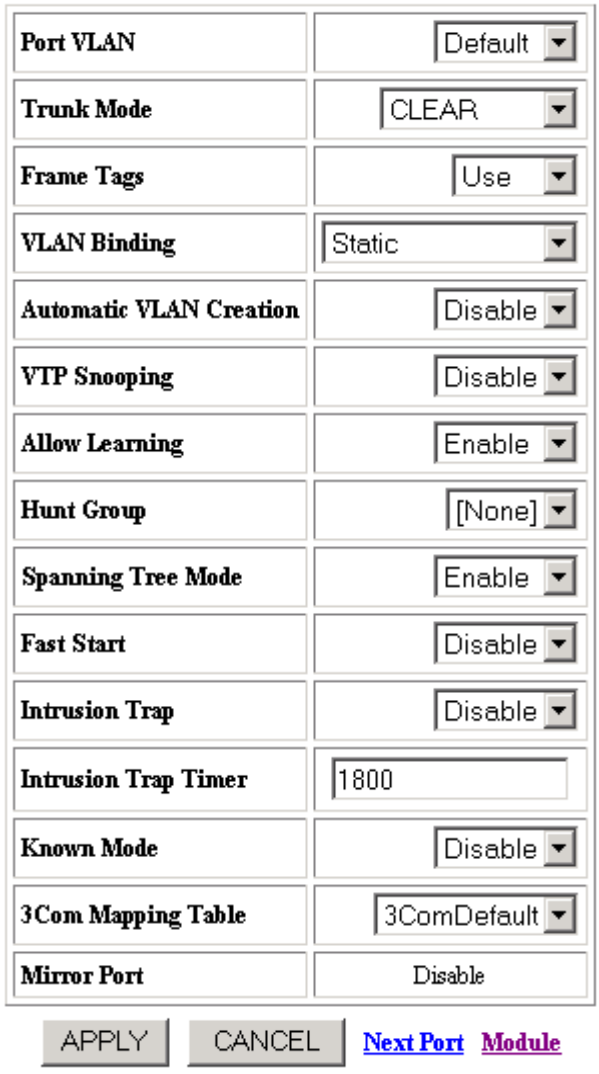
Module Number 5

| Links | Port | Name | Port VLAN | VLAN Classification | Trunk Mode | Hunt Group | STAP Mode | MAC Address |
|---|---|---|---|---|---|---|---|---|
| Port Statistics VLANs | 5.1 | Port 5.1 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:86 |
| Port Statistics VLANs | 5.2 | Port 5.2 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:87 |
| Port Statistics VLANs | 5.3 | Port 5.3 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:88 |
| Port Statistics VLANs | 5.4 | Port 5.4 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:89 |

Prev Module Next Module Modules All Module Switch Ports Configuration

3. Select the **port** in the **Name** column on which you want to enable VTP Snooping throughout the switch. The **Switch Port Configuration** window opens for that port (see Figure 4-27).

*Figure 4-27. Switch Port Configuration Window with VTP Options*



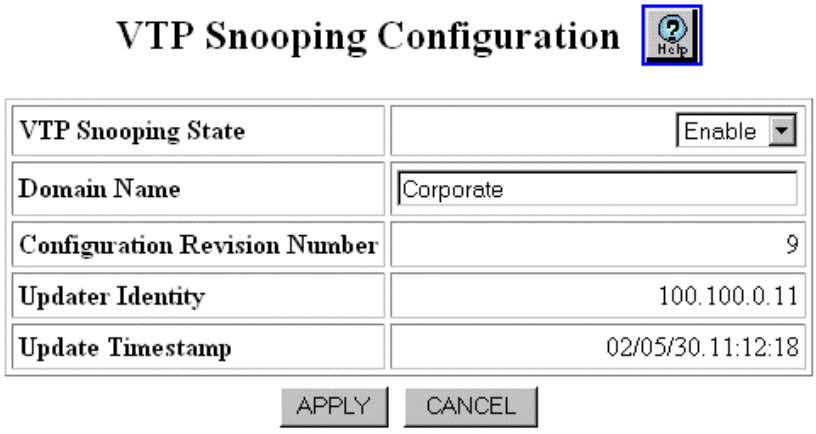

4. Select either **IEEE 802.1Q** or **Multi-layer** from the **Trunk Mode** pull-down menu to match the setting of the trunk mode for the switch port at the other end of the link.

5. Select **Enable** from the **VTP Snooping** pull-down menu. This enables VTP snooping on the switch port.

6. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

7. Select **VTP Snooping** from the **L2 Switching** > **VLANs** folder on the Web Agent window. The **VTP Snooping Configuration** window opens (see Figure 4-28).

*Figure 4-28. VTP Snooping Configuration Window*




8. Refer to Table 4-8 and configure the **VTP Snooping** parameters.

*Table 4-8. VTP Snooping Parameters*

| Parameter | Definition |
|---|---|
| **VTP Snooping State** | Select Enable to enable VTP snooping globally for the switch. The default value is **Disable**.<br>**Note:** Enabling or disabling VTP Snooping does not clear any learned VTP information. |
| **Domain Name** | Enter the name associated with the Cisco VTP Domain. The default is Null (not set). Changing this parameter automatically clears the learned VTP information (the remaining parameters in this table).<br>**Note:** The domain name is automatically learned from a Cisco VTP switch provided both the Domain Name is Null and the VTP Snooping State is enabled on the switch. |
| **Configuration Revision Number** | Displays the VTP snooping configuration revision number associated with the last successful VTP configuration update on the switch.<br>**Note:** VLANs are only be learned by VTP Snooping when a received VTP message has a Configuration Revision Number greater than this learned value. |

*Table 4-8. VTP Snooping Parameters continued*

| Parameter | Definition |
|---|---|
| **Updater Identity** | Displays the IP address of the Cisco switch that initiated the VTP configuration update. |
| **Update Timestamp** | Displays the date and time that the Cisco switch initiated the VTP configuration update. The format of the timestamp is "yy/mm/dd.hh:mm:ss", where yy/mm/dd represents the year, month, and day and hh:mm:ss represents the hours, minutes, and seconds. |

9. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Using the CLI

To configure VTP snooping using the CLI, enter the following command in Configure mode:

```
<configure># set vtp-snooping enable
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# 5 Configuring Port Parameters

## Overview

The following information and procedures are provided in this chapter and are common to both layer 2 and layer 3 module configuration:

- Two Categories of Port Parameters
- Configuring Physical Port Parameters
- Configuring Switch Port Parameters
- GBIC Identification
- Network Error Detection and Recovery
- Internal Error Detection and Recovery

## Two Categories of Port Parameters

The system has two categories of port settings:

- **Physical port parameters** — Allows you to set up rules that guide the system's physical layer interaction (for example, enable/disable, speed, auto-negotiation).
- **Switch port parameters** — Allows you to specify how the port participates in switching (for example, VLAN mode, trunking).

The following sections explain some of the Avaya P550R/P580/P880/P882 Multiservice switch features and how to configure the ports.

# Physical Port Features

This section describes the following features that are available when configuring the physical parameters on the ports:

- Autonegotiation
- Flow Control

## Auto-negotiation

Autonegotiation is an extension of the link test methods used by 10Base-T and 10Base-FL to verify the integrity of the link between devices. Autonegotiation advertises a device's abilities by encoding a 16-bit data packet, called a link code word (LCW), within a burst of 17 to 33 link pulses, called a fast link pulse (FLP) burst. FLP bursts have an approximate duration of 2 µs and are transmitted in 16.8 µs intervals (the same interval as for the normal link pulses used by 10Base-T and 10Base-FL).

However, this does not hold true for the Half Duplex/Full Duplex (HD/FD) selection. If a non-autonegotiating device running FD is connected to a negotiating device, the negotiating device runs at HD, and the link does not operate properly.

*** Note:** A Gigabit Ethernet device negotiates at HD or FD, speed is always one Gigabit.

M5520-TX (P/N M5520-100TX) boards manufactured with a Quality Phy do not auto-negotiate with Xircom brand adapter cards. If you have this problem, disable auto-negotiation on the affected ports, and set the port speed and duplex state manually.

You may experience difficulties with auto-negotiation between some releases of the 10/100Base-TX Module (M5510-100TX, M5520-100TX, M5510R-100TX, M5512R-100TX) and adapter cards using physical interfaces manufactured by National Semiconductor. The symptom is loss of connectivity. If you do. do one of the following:

- Disable auto-negotiation
- Use a patch cable that is longer that 5 meters

*** Note:** The factory default for the National Phy Mode is **Enable**.

The LCW contains two fields (the selector field and the technology ability field), which together serve to identify a device's capabilities.

It may seem that because the FLP and the normal link pulse use the same interval at the same frequency, older devices may not be compatible with auto-negotiation. This is, however, not the case. For example, a 10Base-T device that does not have auto-negotiation capabilities sees FLP bursts simply as a link test signal. A 10Base-T device will respond to the FLP burst with its usual normal link pulse signal. At the other end of the link, a 10/100-capable device will recognize normal link pulse and choose 10Mbps mode operation.

Auto-negotiation attempts to find the greatest common denominator for the two devices on the link in the following order of preference:

1. 100Base-TX full-duplex
2. 100Base-T4
3. 100Base-TX
4. 10Base-T full-duplex
5. 10Base-T half-duplex

*** Note:** T4: 100 Mbps with 8B/6T coding scheme

Once the greatest common denominator of settings is determined, each device equipped with auto-negotiation will configure itself automatically. In certain cases where automatic configurations are not desired, auto-negotiation provides a way for these settings to be overridden manually.

*** Notes:** Auto-negotiation should be disabled only on 50-series modules that have remote fault detection enabled. Do not disable Auto-negotiation on 80-Series gig links.

## Flow Control

There are three flow control options on 10/100 Ethernet ports:

- Disable
- Enable
- Enable with Aggressive Backoff

There are four flow control options on Gigabit Ethernet Ports.

- Disable
- Enable
- Enable – Send Only
- Enable – Respond Only

The "Disable" option disables flow control (the default).

The "Enable" option enables IEEE802.3X (XOFF/XON) Flow Control on the line. The Avaya Multiservice Switch is the sender of pauses based upon inbound traffic and the Avaya Multiservice Switch is the receiver of pauses based upon outgoing traffic (and the ability of attached equipment to use the protocol).

With Gigabit links, you can:

- Enable IEEE802.3X for both send and receive (the “Enable” setting)
- Only send pause (XOFF/XON) signals (the “Enable – Send Only” option)
- Only respond to the pause signals (the “Enable – Respond Only” option).

With 10/100 links you can use the "Enable with Aggressive Backoff" option to enable Active Backpressure (creation of a collision) on a link. Active Backpressure only applies to HD links so that when a 10/100 link is in FD, options 2 and 3 are identical.

Refer to Table 5-1 lists the gigabit modules that do not support auto negotiation:

***Table 5-1. Gigabit Modules not Supporting Autonegotiation***

| Gigabit Module Model Number | Hardware Revision |
|---|---|
| **M5502-1000SX-F** | M or earlier |
| **M5502-1000LX-F** | M or earlier |
| **M5502-1000SLX-F** | F or earlier |
| **M5504-1000SX-F** | H or earlier |
| **M5504-1000LX-F** | H or earlier |
| **M5504-1000SLX-F** | H or earlier |
| | ***1 of 2*** |

*Table 5-1. Gigabit Modules not Supporting Autonegotiation*

| Gigabit Module Model Number | Hardware Revision |
|---|---|
| **M5502R-1000SX-F** | J or earlier |
| **M5502R-1000LX-F** | J or earlier |
| **M5502R-1000SLX-F** | H or earlier |
| | ***2 of 2*** |

*** Note:** If a Gigabit module that does not support the autonegotiation is connected to a device that does, disable autonegotiation to ensure proper operation.

If you enable flow control, the switch manages the inbound buffers with flow control (IEEE 802.1X XOFF, or Backpressure) applied when a high water mark is reached. Thus, no matter which flow control option is chosen, outgoing pauses or backpressure are only applied to the port on which the parameter is set based upon the inbound traffic for that port in the default queuing mode.

Flow control is not applied across the switch itself. Therefore, if you have a server sending data on one port at 100MB and a client receiving the data at 10MB, the switch will not throttle the data at the Server's input based on outgoing buffer backup on the client's port in this default queuing mode.

## Switch Port Features

The Avaya P550R/P580/P880/P882 Multiservice switches all support up to 1000 VLANs and also supports multiple forwarding databases. This means that each VLAN is associated with its own Address Forwarding Table (AFT). Therefore, identical MAC addresses can simultaneously exist on multiple VLANs. The Avaya Multiservice switches provide parameters for configuring VLAN/port associations.

This section provides the following:

- Relationship Between Different Switch Port Parameters
- Assigning VLANs to a Port and Associated Issues
- Setting the Port VLAN attribute in the Switch Port Configuration dialog box. This identifies the VLAN to which all untagged frames received on the port are classified. Note that a port has exactly one Port VLAN. Changing this to a new VLAN removes the port from the old VLAN.

- Setting the VLAN Binding attribute in the Switch Port Configuration dialog box to **Bind to All**. This causes the port to be bound to all VLANs known to the switch (now and in the future). This is not recommended when the switches on both ends of the link function as a router. This setting should be used on links that connect two Layer 2 switches. Refer to the *Avaya P550R, P580, P880, and P882 Multiservice Switch User Guide, Version 5.3.1* for more details
- Setting the VLAN Binding attribute in the Switch Port Configuration dialog box to **Bind to Received**. This causes the port to be bound to all VLANs identified by the VLAN tag in IEEE 802.1Q and Multi-Layer tagged frames received on this port. Consequently, ports are bound to those VLANs that actually have members that are reachable through the port.
- Manually creating a VLAN Switch Port via the Web Agent or CLI.

## Relationship Between Different Switch Port Parameters

Table 5-2 shows the relationship between Port VLAN / Trunk Mode / VLAN Binding parameters when using the VLAN Operational Rules.

*Table 5-2. Relationship Between Switch Parameters*

| VLAN Binding | Trunk Mode | Description |
|---|---|---|
| **Static** | Clear | **Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame.<br>**Forwarding:** Only forward frames to the port for the assigned VLAN.<br>**Egress:** All frames transmitted will be sent with no tagging. |
| **Static** | 802.1Q<br>Multi-layer | **Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame.<br>**Forwarding:** Only forward frames to the port for the assigned VLAN.<br>**Egress:** All frames transmitted out of the port will be tagged using the IEEE 802.1Q/Multi-Layer tag header format. The tag used will be that assigned to the port. |
| Bind to All | Clear | ***NOT RECOMMENDED***<br>**Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame.<br>**Forwarding:** All broadcast frames from all VLANs will be forwarded to the port.<br>**Egress:** All frames transmitted will be sent with no tagging. |
| | | ***1 of 3*** |

*Table 5-2. Relationship Between Switch Parameters*

| VLAN Binding | Trunk Mode | Description |
|---|---|---|
| Bind to All | 802.1Q<br>Multi-layer | **Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the frame's tag header.<br>**Note:** For 802.1q mode: if a tagged frame is received, but the VLAN for that tagged frame does not exist on the switch, that frame will be placed onto the port VLAN assigned to the port. This may cause unicast and broadcast VLAN traffic from other VLANs to be seen on the port VLAN. To avoid this behavior, you can set the port VLAN into the "discard" VLAN which will drop all untagged frames and tagged frames with unknown VLAN IDs. For Multi-layer: if a tagged frame is received, but the VLAN for that tagged frame does not exists on the switch, that frame will be dropped. **Forwarding:** All broadcast frames from all VLANs will be forwarded to the port.<br>**Egress:** All frames transmitted out of the port to be tagged using the IEEE 802.1Q/Multi-Layer tag header format. The tagged used will be that of the VLAN in which the frame was received. |
| | | ***2 of 3*** |

*Table 5-2. Relationship Between Switch Parameters*

| VLAN Binding | Trunk Mode | Description |
|---|---|---|
| Bind to Received | Clear | ***NOT RECOMMENDED***<br>**Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the tag header of the frame.<br>**Forwarding:** All broadcast frames from all VLANs learned on the port will be forwarded.<br>**Egress:** All frames transmitted will be sent with no tagging. |
| Bind to Received | 802.1Q<br>Multi-layer | **Ingress:** Untagged frames are classified to the VLAN associated with the port on which the frame is received. Tagged frames are classified to the VLAN identified by the VLAN tag in the frame's tag header.<br>**Note:** For 802.1q mode: if a tagged frame is received, but the VLAN for that tagged frame does not exist on the switch, that frame will be placed onto the port VLAN assigned to the port. This may cause unicast and broadcast VLAN traffic from other VLANs to be seen on the port VLAN. To avoid this behavior, you can set the port VLAN into the "discard" VLAN which will drop all untagged frames and tagged frames with unknown VLAN IDs.<br>For Multi-layer and 3Com mode: if a tagged frame is received, but the VLAN for that tagged frame does not exists on the switch, that frame will be dropped.<br>**Forwarding:** All broadcast frames from all VLANs learned on the port will be forwarded.<br>**Egress:** All frames transmitted out of the port to be tagged using the IEEE 802.1Q/Multi-Layer tag header format. The tagged used will be that of the VLAN in which the frame was received. |
| | | ***3 of 3*** |

# Assigning VLANs to a Port and Associated Issues

There are two ways to assign VLANs to ports on the Avaya Multiservice Switch. You configure the Port(s) to the VLAN desired for the individual port(s), or entire module. Assigning the VLAN this way enables the port(s) to receive information for the assigned VLAN and causes all untagged frames arriving on this port to be assigned to the specified VLAN. The port(s) will still assign incoming tagged packets to the VLAN indicated by the tag.

In the current release of software, a non-trunk port only supports a single VLAN per port. Multiple VLANs per port is NOT recommended and can have adverse effects on network performance.

The second way is to assign the VLAN to a port is by using the following CLI command in **Enable/Configure** mode:

```
<configure># set VLAN <vlan-id or name> <options>
```

By selecting the VLAN name or VLAN ID, you can bind the selected VLAN to additional ports. When binding VLANs this way, the port is part of the flooding domain of the selected VLAN. This is an alternative to using the binding types “bind to all” and “bind to receive”, that allows you to add a port(s) to a subset of VLANs in the switch.

*** Note:** This configuration should only be used under special circumstances and with the assistance of customer support as undesirable results may occur (e.g. destination unknown unicast storms).

See Chapter 4, “Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping”, for a description of the parameters that will be displayed when viewing VLAN information with the Web Agent and the CLI command syntax.

Although this method of adding VLANs to a port could be thought to support the request for multiple VLANs per port (also referred to as overlapping VLANs), it is NOT recommended on clear (non trunked) ports due to the impact it has on the network. The impact is that destination unknown unicast packets are flooded on the VLAN in which the source host is located. This causes all ports assigned to this VLAN to receive the destination unknown unicast. If enough of these destination unknown unicast packets are being sent it could have a major impact on the network.

The following is an example of a problem with assigning more the one VLAN to a port.

- All PCs and Servers are connected to the Avaya Multiservice Switch 10/100TX switch ports. The following configuring of ports to VLANs are done with the Web Agent.
- PC1 is a member of VLAN1 and is connect to switch Port 1
- PC2 is a member of VLAN2 and is connected to switch Port 2
- SERVER1 is a member of VLAN4 and is connected to switch Port 4

With the *set vlan* CLI command, assign port 1, and port 2 to VLAN4 and also assign port 4 to VLAN1 and VLAN2. Then PC1 and PC2 could communicate with SERVER1 across VLANs without any noticeable problems. However, when PC1 transmits a packet to SERVER1, the following occurs:

- The packet is sent to the Switch
- The switch looks for the MAC address of SERVER1in the Address Forwarding Table for VLAN1 (because this is the actual port VLAN assigned to the port)
- The switch will be unable to find an entry for the MAC address of SERVER1
- The switch will flood this packet to all ports assigned to VLAN1 (regardless of how the VLAN was assigned to the port)

  *** Note:** The only exception to flooding a port is if 'Known Mode' is set to enable on the port, which stops the flooding of destination unknown unicast packets.

If you had many clients/servers on separate VLANs and they tried to communicate over multiple VLANs using this method, you would flood your network with undesired packets, thus slowing your overall network performance. Currently, the best solution is to use a L3 module to route between the VLANs. This would eliminate the broadcast of destination unknown unicast packets.

# Configuring Physical Port Parameters

This section contains the following procedures:

- Configuring Physical Port Parameters on Gigabit Ports
- Configuring Physical Port Parameters on Fast Ethernet Ports
- Using the All Ports Configuration Window

## Configuring Physical Port Parameters on Gigabit Ports

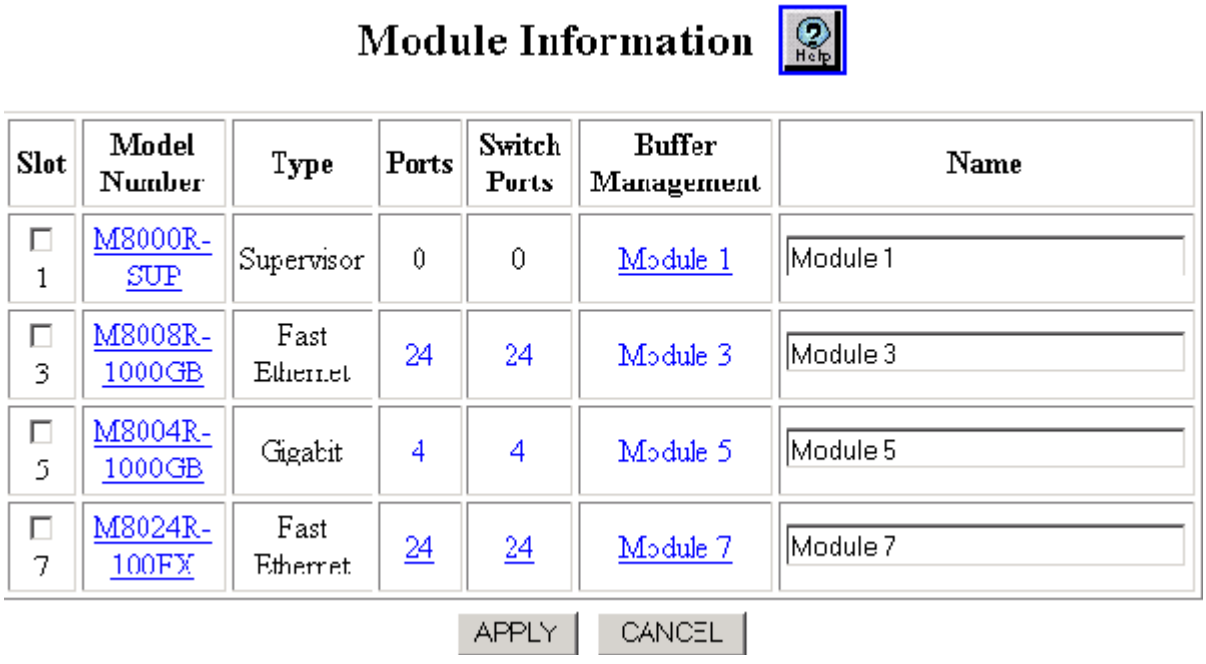
You can configure the physical port parameters on Gigabit ports using either the Web Agent or the CLI.

### Web Agent Procedure

To configure ports on a gigabit module using the Web Agent:

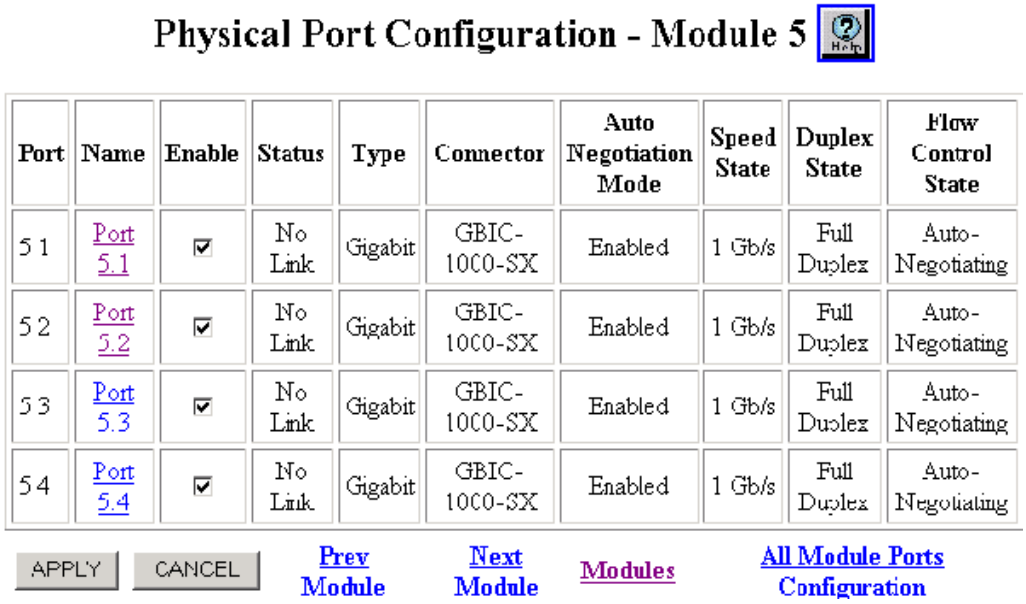
1. Select **Configuration** from the **Modules & Ports** group on the Web Agent window. The Module Information dialog box opens (Figure 5-1).

***Figure 5-1. Module Information Dialog Box***




2. Select the port from the **Ports** column for the Gigabit module that you want to configure. The Physical Port Configuration dialog box for that module opens (Figure 5-2).

*Figure 5-2. Physical Port Configuration Dialog Box for the Gigabit Ethernet Module*



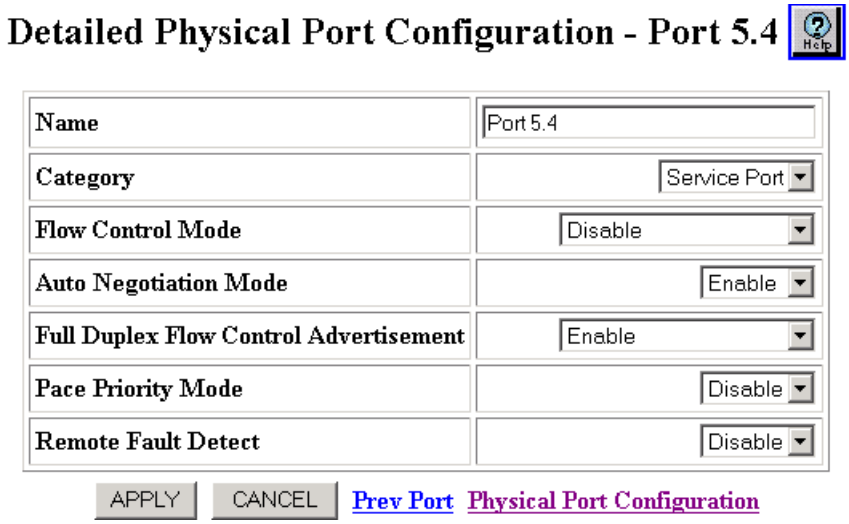

3. Click the checkbox in the **Enable** column to enable a port. A checkmark displays.

   *** Note:** If the port is already enabled (checkmark is visible), and you want to disable the port, click the box to Disable the port (checkmark vanishes).

4. Click **APPLY** to save your settings, or **CANCEL** to restore previous settings.

5. Select the port name from the **Name** field. The **Detailed Physical Port Configuration** dialog box opens (Figure 5-3

*Figure 5-3. Detailed Physical Port Configuration Dialog Box for Port on Gigabit Ethernet Module*




6. Enter a port name in the **Name** field, if desired, or use the default name supplied

7. Select one of the following from the **Category** field pull-down menu:

   — **User Port i**f this is an end-station port

   — **Service Port** if this is a trunk port.

8. Select one of the following options from the **Flow Control Mode** field pull-down menu:

   **Enable** – Set flow control to prevent buffer overflows.

   **Disable** – When flow control is causing congestion in other areas of the network.

   **Enable (Send Only)** – Set flow control to prevent buffer overflows on sent traffic.

   **Enable (Respond Only)** – Set flow control to prevent buffer overflows on respond traffic.

9. Select **Enable** from the **Auto Negotiation Mode** field pull down menu

10. Select **Enable** from the **Full Duplex Flow Control Advertisement** field pull down menu

11. Select **Enable** from the **Pace Priority Mode** field pull down menu to recognize and use 3Com's PACE priority mechanism.

12. Select **Enable** from the **Remote Fault detect** field pull down menu to detect

13. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

Refer to Table 5-3 provides a more detailed description of the Detailed Physical Port dialog box parameters.

***Table 5-3. Detailed Physical Port Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Name** | A user-definable name for this port (possibly a drop connection name or the name of the station or other device connected to the port). |
| **Category** | The **User Port** option is intended for use with switch connections to end user nodes. It is intended for use with switch connections to servers or other switches.<br>The **Service Port** allows the switch to generate both *log messages* and *alarm messages* (traps). The User Port only generates log messages. This prevents your network management station from being overwhelmed by port up/down messages that result from users turning workstations on and off. |
| **Flow Control Mode** | Setting this field determines if the IEEE 802.3z pause control is to be used on this port. The pause mechanism allows the port to stop a sending station from sending more packets if the receiving port's buffers are full. This helps prevent lost or dropped packets.<br>This feature is recommended for use primarily on end station connections. Using this feature on trunk ports can cause unnecessary congestion on the network. |
| | ***1 of 2*** |

*Table 5-3. Detailed Physical Port Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **PACE Priority Mode** | Determines if the port detects 3Com's copyrighted PACE format as packets pass through the port. PACE allows a packet's priority (higher priority packets move through the switch faster) to be set at the adapter. |
| **Remote Fault Detect** | Remote Fault detect, allows a Gigabit port at one end of a link to signal status to the other end of the link, even in the event that it may not have an operational receive link. This feature is useful only when half of a point-to-point link is lost.The remote fault detection should be enabled on both ends of a switch to switch connection, in two cases. First, when two Gigabit ports are connected that do not support auto-negotiation. The second case is when there is a mis-match between Gigabit ports, one supports auto-negotiation and the other does not.<br>**Note:** Auto-negotiation and remote fault detection can not be enabled at the same time.Aut0-negotiation must be disabled in order to enable remote fault detection. When auto-negotiation is enabled, remote fault detection is automatically disabled. |
| | ***2 of 2*** |

## CLI Command

To configure ports on a gigabit module using the CLI, enter the following command from Configure mode:

```
<configure># set port <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for more details about this command.

*** Note:** When a port on an 80-Series Gigabit Ethernet module is disabled, the port link light blinks continuously. In versions earlier than v5.2.10, the link light extinguished when the port was disabled.

Loopback tests on ports may fail when traffic is present on the link at startup.

# Configuring Physical Port Parameters on Fast Ethernet Ports

You can configure ports on a Fast Ethernet module using either the Web Agent or CLI commands.

## Web Agent Procedure

To configure ports on a Fast Ethernet module using the Web Agent:

1. Select **Configuration** from **Modules & Ports** group on the Web Agent window. The Module Information dialog box opens (Figure 5-1).
2. Select the checkbox in the **Slot** column next to the Fast Ethernet module to change the Name field, if desired, change the module name then **Click** the APPLY button.
3. Select the number in the **Ports** column for the Fast Ethernet module that you want to configure. The Physical Port Configuration window opens (Figure 5-4).

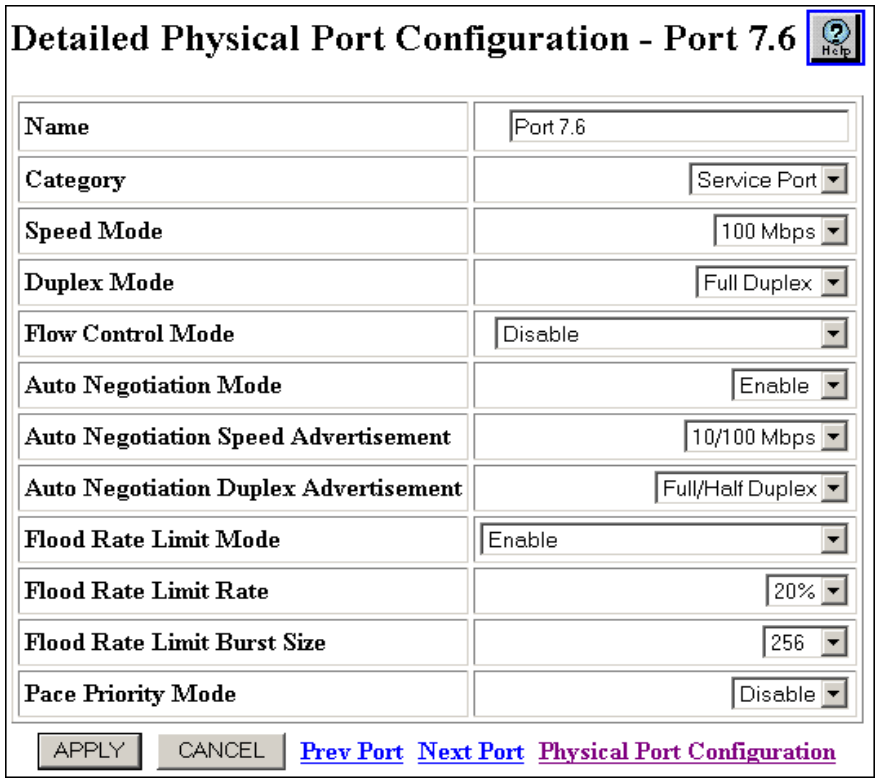
***Figure 5-4. Physical Port Configuration Window for the Fast Ethernet Module installed in Slot 3 (partial view)***

**Physical Port Configuration - Module 3** Help

| Port | Name | Enable | Status | Type | Connector | Auto Negotiation Mode | Speed State | Duplex State | Flow Control State |
|---|---|---|---|---|---|---|---|---|---|
| 3.1 | Port 3.1 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 3.2 | Port 3.2 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 3.3 | Port 3.3 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |
| 3.4 | Port 3.4 | ☑ | No Link | 10/100 Tx | RJ45 | Enabled | Auto-Negotiating | Auto-Negotiating | Disabled |

4. By default the checkbox is checked in the **Enable** column. To change the enable remove the check in the checkbox.
5. If you change the enable checkbox **Click APPLY** to save your settings, or **CANCEL** to restore previous settings.
6. Select a port name from the **Name** field (for example, Port 6.1). The **Detailed Physical Port Configuration** dialog box for that port opens (Figure 5-5).

*Figure 5-5. Detailed Physical Port Configuration Dialog Box for Port on Fast Ethernet Module*




7. Enter a port name in the **Name** field, if desired or use the default name.

8. Select one of the following from the **Category** field pull-down menu:

   — **User Port i**f this is an end-station port

   — **Service Port** if this is a trunk port.

9. Select a speed (**10 Mb/s** or **100 Mb/s**) from the **Speed Mode** field pull down menu, If you want to set the port speed manually. If want the port to autonegotiate, you can ignore this field.

   *** Note:** This feature is only available for 10/100 TX modules.

10. Select a duplex mode (half-duplex or full-duplex) from the **Duplex Mode** field pull-down menu if you want to manually set the port's duplex mode. You do not have to select a duplex mode if you set the port to autonegotiate.

**11.** Select one of the following from the **Flow Control Mode** field pull-down menu:

**Enable** – Sets flow control to prevent buffer overflows.

**Disable** – Disables flow control when it is causing congestion in other areas of the network.

**Enable (with Aggressive Backoff)** – Limits the size of flow control burst on TX and FX ports.

**12.** Select **Enable** from the **Auto Negotiation Mode** field pull-down menu to enable Auto Negotiation.

*** Note:** This feature is only available for 10/100 TX modules.

Auto Negotiation works best when the port or device on the other end of the connection is also set to Auto Negotiation. If you are having problems with Auto Negotiating connections, manually set the modes using the CLI. See the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for more information.

**13.** Select a speed from the **Auto Negotiation Speed Advertisement** pull- down menu. The options are 10Mbps, 100Mbps. or 10/100Mbps.

**14.** Select a duplex option from the **Autonegotiation Duplex Advertisement** field pull-down menu. The options are Full/Half Duplex and Half Duplex).

*** Note:** The Speed and Duplex features are only available for 10/100 TX modules.

The switch sends the Speed and Duplex advertisement values to the device on the other end of the connection at the start of the auto-negotiating process. In general, the defaults are best, but there may be situations when you want to fix one setting, but allow the other setting to auto-negotiate.

**15.** Select one of the following from the **Flood Rate Limit Mode** pull-down menu:

**Enable** – If you want this port to limit the number of unknown unicast and multicast (flooded) packets it tries to forward

**Disable** – If you do not want this port to limit the number of unknown unicast and multicast packets it tried to forward

**Enable (include Known Multicasts)** – If you want to optionally include known multicast packets in this percentage to further decrease the possibility of the port's output buffer being overwhelmed.

16. Select the percentage of a port's traffic that can be unknown unicast and broadcast packets from the **Flood Rate Limit Rate** field pull-down menu.

    *** Note:** Set this value lower if the port is having overflow problems.

17. Open the **Flood Rate Limit Burst Size** pull down menu.

18. Select a packet limit for the number of packets allowed in a single burst. The values are 1 to 2048.

    *** Note:** Set this value lower than 1024 (the output buffer's capacity) for Fast Ethernet ports. Also set this value lower if the port is experiencing overflow problems.

19. Select **Enable** from the **Pace Priority Mode** pull-down menu if you want this port to recognize and use 3Com's PACE priority mechanism.

20. Click **APPLY to** save your changes, or **CANCEL** to restore previous settings.

Table 5-4 describes in detail the Fast Ethernet port parameters:

*Table 5-4. Fast Ethernet (10/100) Port Parameters*

| Parameter | Definition |
|---|---|
| **Name** | Enter a user configurable name for this port (possibly a drop connection name or the name of the station or other device connected to the port). |
| **Category** | Select either User Port or Service Port.<br>• The **User Port** is intended for use with switch connections to end user nodes.<br>• The **Service Port** is intended for use with switch connections to servers or other switches. The Service Port allows the switch to generate both *log messages* and *alarm messages* (traps). The User Port only generates log messages, preventing your network management station from being overwhelmed by port up/down messages that result from users turning workstations on and off. |
| **Speed Mode** | Select the speed of the port manually (to either 10 or 100 Mb/s). **If auto-negotiation is enabled, this setting is ignored.** |
| **Duplex Mode** | Select the port duplex mode (half- or full-duplex). **If auto-negotiation is enabled, this setting is ignored.** |
| **Flow Control Mode** | Determines if flow control is used on this port. For half-duplex links, active backpressure jams the sending Ethernet channel until the port's buffers can receive more packets. This prevents lost or dropped packets.<br>For full-duplex links, IEEE 802.3z pause control allows the port to stop a sending station from sending more packets if the receiving port's buffers are full.<br>For TX and FX ports, there is an additional option for Enable with Aggressive Backoff. This option limits the size of the bursts.<br>Flow Control is recommended for use primarily on end-station connections. Using this flow control on trunk ports can cause unnecessary congestion on the network. |
| | ***1 of 2*** |

*Table 5-4. Fast Ethernet (10/100) Port Parameters*

| Parameter | Definition |
|---|---|
| **Auto Negotiation Mode** | Select the port to auto-negotiate a speed and duplex mode. Auto-negotiate works best when the connection on the other end of the link is set to auto-negotiate as well. If you set a port to auto-negotiate, and the connection is not successful, set the port speed and duplex mode manually. |
| **Auto Negotiation Speed Advertisement** | Determines what information the port advertises when it starts auto-negotiating. In most cases, **10/100** are the best settings, but there may be cases when you want to auto-negotiate one parameter, while keeping the other fixed. |
| **Auto Negotiation Duplex Advertisement** | Determines what information the port advertises when it starts auto-negotiating. In most cases, **Half/Full** are the best settings, but there may be cases when you want to auto-negotiate one parameter, while keeping the other fixed. |
| **Flood Rate Limit Mode** | Prevents the switch from overwhelming the output buffer on lower-speed ports by placing a threshold on the percentage of port traffic that can be flooded packets (unknown unicasts and multicasts).<br>You can also optionally include known multicast packets in this percentage to further decrease the possibility of the port's output buffer that is being overwhelmed. |
| **Flood Rate Limit Rate** | Determines the percentage of a port's forwarded traffic that can be unknown unicast and multicast (flooded). Lower this value if the port has overflow problems. |
| **Flood Rate Limit Burst Size** | Enter a value for the limit of packets allowed in a single burst. Accepted values are 1 to 2048. For Fast Ethernet ports, set this value lower than 1024 (output buffer capacity). Lower this value if the port has overflow problems. |
| **Port PACE Priority** | Select Enable to allow the port to detect 3Com's proprietary PACE format as packets pass through the port. PACE allows a packet's priority (higher priority packets move through the switch before lower priority packets) to be set at the adapter. |
| | ***2 of 2*** |

### CLI Command

To configure ports on a Fast Ethernet module using the CLI, enter the following command from Configure mode:

```
<configure># set port <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for more details about this command.

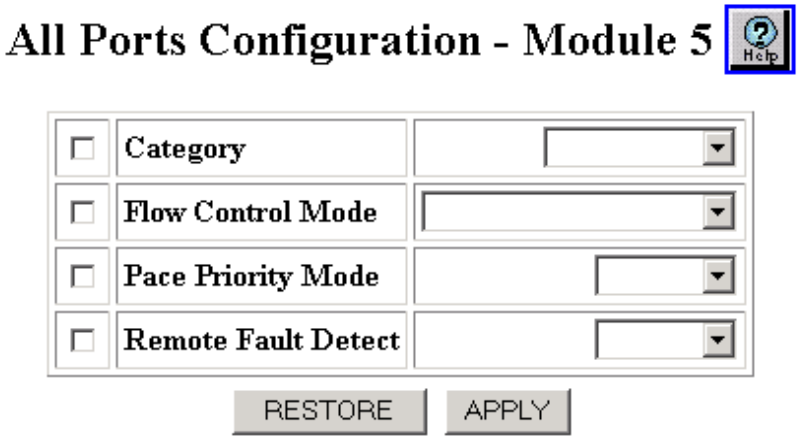
## Using the All Ports Configuration Window

You can apply the same parameter settings on all of a module's ports using the All Ports Configuration dialog box.

To configure all ports on a module:

1. Select **Configuration** from the **Modules & Ports** group on the Web Agent window. The Module Information dialogue box opens (Figure 5-1).
2. Select the port number from the **Ports** column for that module. The Physical Port Configuration dialog box for that module opens (Figure 5-2 for Gigabit modules and Figure 5-4 for 10/100 modules).
3. **Select All Module Ports Configuration**. The All Ports Configuration dialog box opens (Figure 5-6).

***Figure 5-6. All Ports Configuration Dialog Box***



4. Refer to "Configuring Physical Port Parameters on Gigabit Ports" and "Configuring Physical Port Parameters on Fast Ethernet Ports" earlier in this chapter to configure the port parameters.

5. Click **APPLY** to save your changes, or **Restore** to restore previous settings.

# Configuring Switch Port Parameters

This section contains the following procedures:


- Configuring Switch Port Parameters
- Configuring Fast Start Mode
- Using the All Module Ports Configuration Window
- Viewing Switch Port Parameters


## Configuring Switch Port Parameters

You can configure how each switch port performs its switching functions (for example, VLAN parameters, hunt group assignments, trunk mode, and frame tag scheme) through the switch port parameters.

You can configure switch port parameters using either the Web Agent or the CLI.

**CAUTION**

Before changing the VLAN that a port is assigned to, you must remove the port from the hunt group that the port is assigned to. Do *not* attempt to change the VLAN and remove the port from the hunt group simultaneously. If you attempt to change the VLAN that the port is assigned to and remove the port from the hunt group simultaneously, the switch assigns all ports in the hunt group to the new VLAN.

### Web Agent Procedure

To configure switch port parameters using the Web Agent:

1. Select **Configuration** from the **Modules & Ports** group on the Web Agent window. The **Module Information** dialog box opens (Figure 5-1).

2. Select the switch ports for a module from the **Switch Ports** column. The Switch Ports dialog box opens (Figure 5-7).

*Figure 5-7. Switch Ports Dialog Box*

**Switch Ports**

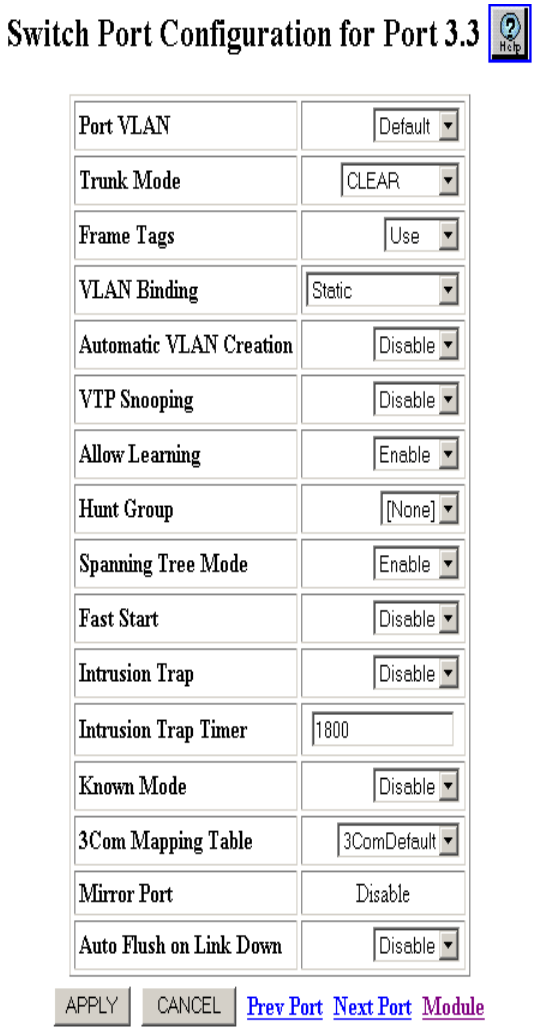
**Module Number 5**

| Links | Port | Name | Port VLAN | VLAN Classification | Trunk Mode | Hunt Group | STAP Mode | MAC Address |
|---|---|---|---|---|---|---|---|---|
| Port Statistics VLANs | 5.1 | Port 5.1 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:86 |
| Port Statistics VLANs | 5.2 | Port 5.2 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:87 |
| Port Statistics VLANs | 5.3 | Port 5.3 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:88 |
| Port Statistics VLANs | 5.4 | Port 5.4 | Default | Port Based | CLEAR | [None] | Enable | 02:e0:3b:1b:04:89 |

Prev Module Next Module Modules All Module Switch Ports Configuration

3. Select a port name from the **Name** column. The Switch Port Configuration dialog box opens (Figure 5-8).

*Figure 5-8. Switch Port Configuration Dialog Box*




4. Select any VLAN from the **Port VLAN** field pull-down menu. This causes all untagged frames arriving on this port to be assigned to the specified VLAN. The port will still assign incoming tagged packets to the VLAN indicated by the tag.

   *** Note:** Refer to Chapter 4 for VLAN creation.

5. Select an option from the **Trunk Mode** field pull-down menu. The options are **Clear** (default), **IEEE 802.1Q**, **Multi-layer**, and **3Com**. Refer to Table 5-5 for an explanation of these options.

6. Select an option from the **Frame Tags** field pull-down menu. The options are **Use** (default) and **Ignore**. Refer to Table 5-5 for an explanation of these options.

7. Select an option from the **VLAN Binding** field pull-down menu. The options are **Static** (default), **Bind-to-All**, and **Bind-to-Receive**. Refer to Table 5-7 for an explanation of these options.

8. Select **Enable** or **Disable** (default) from the **VTP Snooping** field pull-down menu.VTP is a Cisco proprietary Layer 2 trunk port protocol that is used among Cisco switches, over trunk ports, to maintain a VLAN configuration consistency across the network.The switch performs VTP operations when connected to a Cisco switch's trunk that has VTP enabled. The switch queries its Cisco peer for its VLAN configuration. It also learns Cisco VLAN configurations from received Cisco message.

9. Select **Enable or Disable** (default) from the **Automatic VLAN Creation** field pull-down menu. This automatically creates a VLAN each time the port receives a frame from an unknown VLAN.

10. To **Allow Learning**, select **Disable** from the field pull-down menu. This prevents the port from learning new MAC addresses. This feature can be useful for security.

    *** Note:** If you want to allow a port to learn new addresses, reselect Enable. For example, you can set this parameter to Disable, then add a static MAC address entry for this port.

    If you do not select Disable before you add a static MAC address, Unicast flooding can result.

11. Select a Hunt group from the **Hunt Group** field pull-down menu. Refer to Chapter , "Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping" for more information on hunt groups.

12. Select **Disable** from the **Spanning Tree** field pull-down menu to keep STP from running on this port. Reselect **Enable** to run STP on this port.

13. Select **Enable** from the **Fast Start** field pull-down menu to allow Fast Start mode ports to begin forwarding traffic without waiting for STP negotiation to complete. Fast start eliminates the listening and learning waiting times. Ports immediately enter the forward state. Reselect Disable to prevent traffic from being forwarded.

14. Set the **Intrusion Trap** field to **Enable** to enable Intrusion Trap.

15. Adjust the **trap timer,** if desired.

16. Select **Enable** from the **Known Mode** field pull-down menu to suppress any packets that have unknown unicast destination addresses and are flooded to this port.

    For example, if a known end-station or file server is connected to the port, there's no need to flood unknown unicasts to that port. You must manually enter a static MAC address for the station actually attached to the port. Reselect Disable to prevent the suppressing of packets.

17. Select **3Com Default** from the **3Com Mapping Table** field pull-down menu to specify how incoming tagged frames from 3Com equipment are mapped to VLANs. Refer to "Assigning Ports to VLANs", in Chapter 4 for more information.

18. **Mirror Port** Always disabled

19. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

*** Note:** Do not enable Automatic VLAN Creation and VTP Snooping at the same time.

Table 5-5 describes the Switch Port Configuration dialog box parameters.

***Table 5-5. Switch Port Configuration Parameters***

| Parameter | Definition |
|---|---|
| **Port VLAN** | Specifies the VLAN assignment for this port. |
| **Trunk Mode** | Select the appropriate VLAN trunking format to make the port a trunk, or Clear (default) if you do not want the port to be a trunk. The trunk formats are IEEE 802.1Q, Multi-Layer, and 3Com. |
| **Frame Tags** | Select Ignore if you do not want to use received Frame VLAN tags. Use is the default.<br>**Note:** If you select ignore, the received frames are bound to the port's default VLAN. |
| **VLAN Binding** | Select the port's outgoing VLAN binding type. Refer to Table 5-7 for more information on VLAN binding options. |
| **Automatic VLAN Creation** | Select Enable to automatically create a VLAN each time the port receives a frame from an unknown VLAN. Disable is the default. |
| | ***1 of 2*** |

*Table 5-5. Switch Port Configuration Parameters*

| Parameter | Definition |
|---|---|
| **VTP Snooping** | Select Enable to allow VTP Snooping on this port. Disable is the default. |
| **Allow Learning** | Select Disable to keep the port from learning new MAC addresses and forwarding them to the Supervisor module to be added to the VLANs AFT. Enable is the default.<br>**Note:** If a MAC address is moved to a different VLAN, it will co-exist in AFTs, one entry for each VLAN (This is a benefit of having multiple forwarding databases). |
| **Hunt Group** | Select a hunt group for which this port will be a member. None is the default. |
| **Spanning Tree Mode** | Select Disable to remove STP on this port. Enable is the default. |
| **Fast Start** | Select Enable for fast start on this port. Disable is the default. |
| **Intrusion Trap** | Specifies whether or not the port will insert an intrusion trap. |
| **Intrusion Trap Timer** | Specifies the time when the intrusion trap will occur. |
| **Known Mode** | Specifies whether or not the port will broadcast traffic with an unknown destination in the address forwarding table (e.g., destination unknown unicast packets). Disable allows broadcast traffic with an unknown destination to be transmitted over the port (default). Enable allows the port to only forward frames with known destinations in the address forwarding table. |
| **3Com Mapping Table** | Select how incoming tagged frames from 3Com equipment are mapped to Avaya VLANs. The default value is 3ComDefault. |
| **Mirror Port** | Displays the status of the mirror port (enabled or disabled). This is a Fast Ethernet only option. |
| **Auto Flush on Link down** | Select enable Auto Flush for a port to mark all entries learned on that port invalid if the link to that port fails. |
| | ***2 of 2*** |

## Example

Refer to Table 5-6 as an example of the recommended switch port settings for a Cisco Catalyst 5000™.

***Table 5-6. Example 1. Trunk to Cisco Catalyst 5000™***

| Parameter | Recommended Setting |
|---|---|
| **Port VLAN** | **Default** - Causes untagged packets to be assigned to the default VLAN. |
| **Trunk Mode** | **Multi-layer** - Causes the port to send frames using the multi-layer format. |
| **VLAN Binding** | **Bind to All** - Binds the port to all VLANs known to the switch. |
| **Automatic VLAN Creation** | **Enable (Disable if using VTP Snooping)** - Causes the switch to learn new VLAN IDs that arrive at the port, and then bind the port to these VLANs. |
| **VTP Snooping** | **Enable** - Causes the switch to update its VLANs as they are created, deleted, or changed on the Catalyst. |
| | |

## CLI Command

To configure switch ports using the CLI, enter the following command from **Configure** mode:

```
<configure># set port <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3*for more details about this command.

*** Note:** See the examples later in this section for recommendations on how to set particular trunk port connections.

Refer to "VLAN Operation" in Chapter 4 for more information on creating VLANs.

You can configure port VLAN parameters using either the Web Agent or the CLI.

# Automatic VLAN Creation

Automatic VLAN creation is done by enabling the 'Automatic VLAN Creation' parameter on an individual port under the 'Module & Ports'>Configuration >Switch Ports > name menu. With this parameter enabled, the port will automatically create a VLAN each time it receives a frame from an unknown VLAN ID in received IEEE 802.1Q and Multi-Layer tagged frames.

*** Note:** The automatic VLAN creation feature does not create entries in 3Com Mapping Tables.

When a VLAN is created automatically the VLAN name and VLAN ID are derived from the received tagged frame. The VLAN name will be created as "**autoVlan* [VLAN ID]". The VLAN ID will be identical to the VLAN ID of the received tagged frame. As with all VLANs, the VLAN name may be modified to something more descriptive.

Refer to Table 5-8 shows the Avaya P550R/P580/P880/P882 Multiservice switch VLAN table. The VLANs 'Default' and 'Discard' are permanent VLANs assigned to every switch. VLAN 'Net90' is a manually created VLAN, while VLAN '*autoVlan1001' was created automatically by software.

Table 5-7 describes the **VLAN Binding** field pull-down menu options.

***Table 5-7. VLAN Binding Field Pull-Down Menu Options***

| Option | Definition |
|---|---|
| **Static** | Assigns VLAN membership manually, using the VLAN Switch Ports page described in "*Creating and Implementing VLANs*", in Chapter 4. |
| **Bind to All** | Binds this port to all VLANs known to the switch. This is an appropriate mode for switch-to-switch connections.<br>**Note:** When a tagged IEEE 802.1Q packet arrives on a port that is set to bind to all and the VLAN does not exist on the switch, the packet is forwarded on to the VLAN assigned to the port default VLAN for that port. To prevent unintended forwarding of unknown VLAN traffic to the port's default VLAN, configure the port default VLAN to Discard. The automatic VLAN creation feature will not work if the port's default VLAN is the discard VLAN, because the switch does not learn for this VLAN. |
| **Bind to Received** | Binds this port to any VLAN it receives traffic from.<br>**Note:** If Automatic VLAN Creation is enabled, the port binds to previously unknown VLANs and a VLAN entry is added to the switch VLAN table. If Automatic VLAN Creation is disabled, the port does not bind to any VLAN unknown to the switch. |

***Table 5-8. Avaya P550R/P580/P880/P882 Multiservice Switch VLAN Table.***

***Table 5-9.***

| Name | ID | Group ID | AFT Index |
|---|---|---|---|
| Default | 1 | 2 | 1 |
| Discard | 4097 | 3 | 3 |
| Net90 | 90 | 90 | 7 |
| *autoVlan100 | 100 | 100 | 11 |

* Automatically created by the switch software
All others created manually

## Automatically Creating VLANs and Frame Tags Parameters

VLANs are created automatically by the switch reading the VLAN tag of all ingress IEEE 802.1Q and Multi-Layer tagged frames. The switch then creates a new VLAN for every new VLAN tag identified. However, if the parameter for 'Frame Tags' is set to "ignore", the switch will ignore the VLAN tags on ingress frames. The switch assumes that all ingress frames belong to the 'Port VLAN'. Therefore, no new VLANs will ever be created automatically.

## Automatic Binding of VLANs to Ports

When a VLAN is either manually or automatically created, the software may automatically bind the VLAN to a port depending on the setting of the 'Trunk Mode' parameter assigned to the port.

- When a VLAN is created manually the software assigns the VLAN to all ports whose **VLAN Binding** is set to **Bind to All**. No other ports will automatically be assigned when a VLAN is created manually.
- When a VLAN is created automatically the software assigns the VLAN to the port it is received on if that port is set to **Bind to All** and **Bind to Received**. Additionally, software will assign the VLAN to all other ports whose **VLAN Binding** is set to **Bind to All.**

following command from **Configure** mode:

```
<configure># set port VLAN <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for more details about this command.

# Configuring Fast Start Mode

Fast Start mode causes ports to begin forwarding traffic without waiting for the spanning tree negotiation to complete. You may want to set a port to Fast Start mode in the following examples:

- End-station ports that do not need to participate in the full spanning tree negotiation
- Loop-free topologies that do not need spanning tree protocol to resolve redundant connections
- Endstations that require immediate forwarding of traffic in order to receive configuration information, such as IPX clients or DHCP clients.

You can configure Fast Start mode using either the Web Agent or the CLI.

## Web Agent Procedure

To enable Fast Start mode for ports on a module associated with a selected bridge using the Web Agent:

1. Select **Configuration** from the **Modules & Ports** group on the Web Agent window. The Module Information window opens (Figure 5-1).
2. Select the switch port number listed for that module from the **Switch Ports** column. The **Switch Ports** dialog box opens (Figure 5-7).
3. Select the port name for the selected module in the **Name** column if you want to set Fast Start mode on individual ports. The **Switch Port Configuration** dialog box for that port opens (Figure 5-8).
4. Select **All Module Switch Port Configuration** if you want to set fast mode on all ports on a module. The **Switch Port Configuration on All Ports** dialog box for that module opens.
5. Select **Enable** from the **Fast Start** field pull-down menu to allow Fast Start mode on the selected module ports.
6. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

### CLI Command

To configure Fast Start mode for ports on a module associated with a selected bridge using the CLI, enter the following command from Configure mode:

```
<configure># set port fast-start <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for more details about this command.

## Enabling the Auto Flush Feature

### Overview

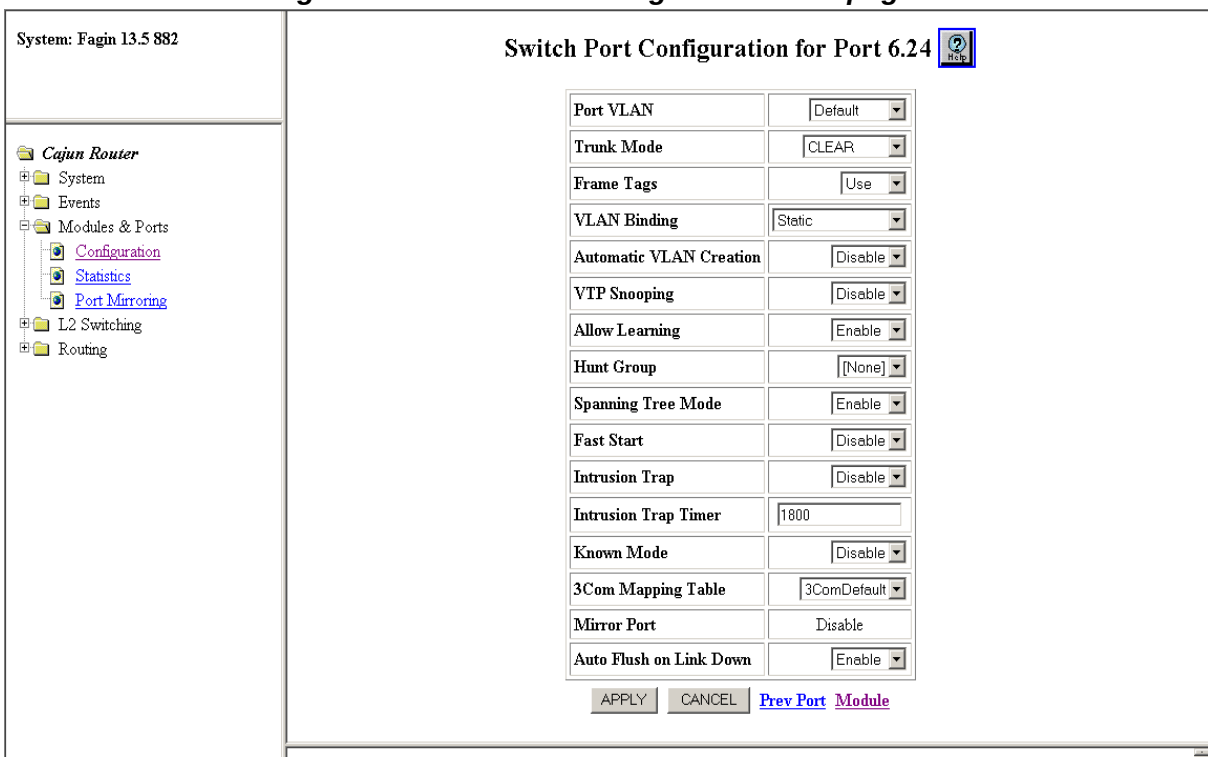
The Auto Flush feature has been added to the switch on both a per-port, and per module basis. When you enable Auto Flush for a port, and the link to that port fails, all entries in the address forwarding table learned on that port are marked invalid. You should enable Auto Flush on all P58x and P88x ports that are participating in a Port Redundancy configuration with a P330.

### Web Agent Procedure

To enable Auto Flush by using the Web Agent, use the following procedure:

7. In the Web Agent navigation pane, expand the **System** > **Modules and Ports** folders.
8. Select the **Configuration** Web Page.
9. In the **Module Information** pane, click the port link in the **Switch Port** column that you want to enable auto-flush for.
10. On the **Switch Ports** web page, click either the port link in the **Name** column that you want to enable auto-flush for, or
11. Click the **All Module Switch Ports Configuration** link if you want to enable auto-flush for all ports within the module.
12. Select **enable** from the **Auto Flush on Link Down** pull-down menu on the **Switch Port Configuration** page.
13. Click **Apply** to save changes, or **Cancel** to exit the Web page without saving your changes.

*Figure 6. Switch Port Configuration Web page*




## CLI Commands

Use the following command to enable Auto Flush on link down:

**set port auto-flush <*module-number*>/<*mod-swport-range*> enable**

Use the following command to disable Auto Flush on link down:

**set port auto-flush <*module-number*>/<*mod-swport-range*> disable**

*** Note:** You must be in Global Configuration mode to enter the **set port auto-flush** commands.

For more information about these commands, see Chapter 19, "Port," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*

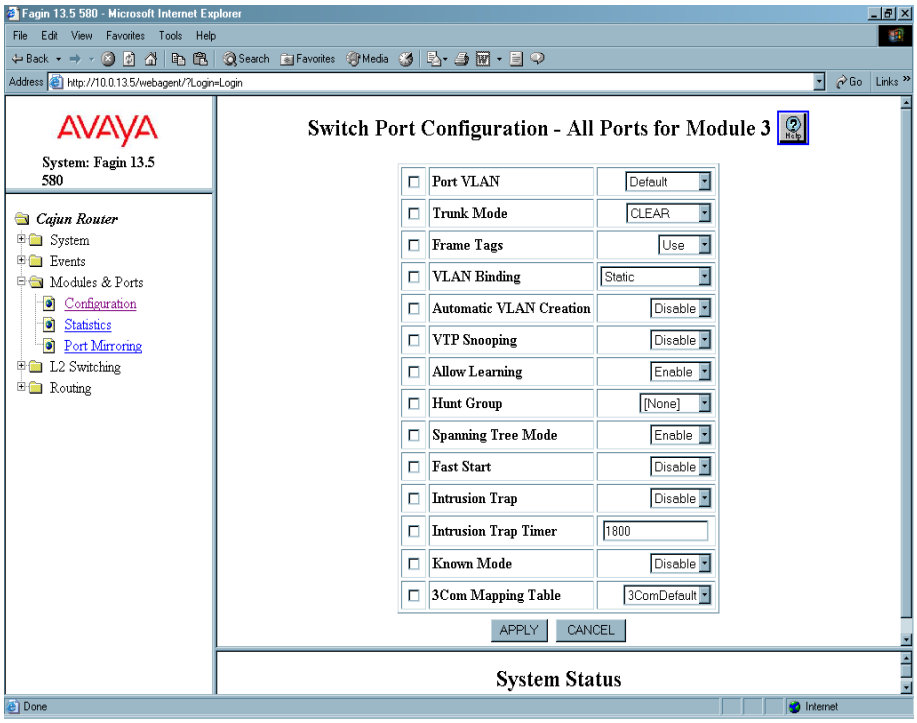
# Using the All Module Ports Configuration Window

The All Ports Configuration window allows you to apply the same parameter settings to all switch ports in a module using a single command.

To set all switch ports in a module using a single command:

1. Select **Configuration from the Modules & Ports group on the Web Agent window**. The **Module Information** dialog box opens (Figure 5-1).
2. Select the switch port number listed for that module from the **Switch Ports** column. The **Switch Ports** dialog box opens (Figure 5-7).
3. Select **All Module Switch Ports Configuration**. The Switch Ports Configuration - All Ports dialog box opens (Figure 6-9).

***Figure 6-9. Switch Ports Configuration - All Ports dialog box***




4. Select the check box next to the field you want to configure.
5. Select an option for the specific field from that fields pull-down menu.

6. Select **Restore** to keep the previous settings or **Apply** to accept the new settings.

# Viewing Switch Port Parameters

You can view switch port parameters through either the Web Agent and the CLI.

## Web Agent Procedure

To view switch port parameters using the Web Agent:

1. **Select** Configuration from the **Modules & Ports group of the Web Agent window**. The **Module Information** dialog box opens (Figure 5-1).
2. Select the switch ports for that module from the **Switch Ports** column. The Switch Ports dialog box opens (Figure 5-7).
3. Refer to Table 6-1 for more information about the **Switch Port** dialog box parameters:

***Table 6-1. Switch Port Parameters***

| Parameter | Definition |
|---|---|
| **Links** | Opens associated windows. |
| **Port** | Displays the port associated with the selected module. |
| **Name** | Displays the port name and opens the Switch Port Configuration window for the selected module. |
| **Port VLAN** | Displays the port VLAN for the selected module. |
| **VLAN Classification** | Displays the port VLAN classification for the selected module. |
| **Trunk Mode** | Displays the port's trunk mode for the selected module. |
| **Hunt Group** | Displays the hunt group of which the port is a member for the selected module. |
| **STAP Mode** | Displays whether the spanning tree algorithm protocol is enabled or disabled for the selected module. |
| **MAC Address** | Displays the port's MAC address for the selected module. |
| | |

4. Select one of the following items listed at the bottom of the screen for more information about the switch ports:
   - **Next/Previous Module** – Displays the next or previous module's switch port parameters.
   - **Modules** – Returns you to the Module Information window.
   - **All Module Switch Ports Configuration** – Opens the Switch Port Configuration All Ports window and configures all ports for the selected module.

### CLI Command

To view switch port parameters using the CLI, enter the following command from Priv mode:

```
> show port [{<mod-num>|<mod-swport-range>}
[...,{<mod-num>|<mod-swport-range>}]]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for more details about this command.

# GBIC Identification

The GBIC Identification feature identifies the type of GBICs that are installed in 80-series gigabit modules with GBIC interfaces. The feature identifies the following types of connectors:

- GBIC SX (short wavelength)
- GBIC LX (long wavelength)
- GBIC LX/LH (long wavelength/long haul)

If any nonstandard connectors are present, the feature identifies them as GBIC LX/LH. You can view this information by using the Web Agent, CLI, or SNMP.

### Web Agent Procedure

To use the Web Agent to view the type of GBICs that are connected to the modules in your switch, open the Physical Port Configuration Web page. The type of GBIC that is connected to each port is displayed in the **Connector** field on this Web page.

To open the Physical Port Configuration Web page:

1. Expand the **Modules & Ports** folders.

2. Click **Configuration**.

   The Module Information Web page opens.

3. In the **Ports** column, click the number for the module that you want to view GBIC types for.

   The Physical Port Configuration Web page opens (Figure 5-2 for Gigabit modules and Figure 5-4 for 10/100 modules).

### CLI Command

To use the CLI to view the type of GBICs that are connected to the modules in your switch:

1. Enter either the User, Privileged, or Global Configuration mode.

   *** Note:** For information on how to enter these modes, see "Accessing/Exiting the Command Modes" in Chapter 1, "Overview," of *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3*.

2. Enter the following command:

   **show port physical [{<*mod-num*> | <*mod-swport-range*>} [...,{<*mod-num*> | <*mod-swport-range*>}]]**

   The type of GBIC that is connected to each port is displayed in the `Connector` field.

### SNMP MIB Object

To use SNMP to view the type of GBICs that are connected to the modules, use the MIB objects that are listed in Table 2. These MIB objects are located in **ProminetMib.txt**, version 5.2.

***Table 2. MIB, MIB Object, and OID for GBIC Identification***

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.2 | promPortConnector | 1.3.6.1.4.1.2167.3.6.1.1.1.7 |

# Network Error Detection and Recovery

## Overview

The Network Error Detection and Recovery (NEDR) feature monitors Ethernet CRC errors on Ethernet data ports and compares

the rate of errors that occurs to the threshold values that you set. This feature helps you find the source of the errors and take corrective action if necessary.

This feature monitors the Ethernet CRC errors on Ethernet data ports. At a pre-determined interval, the feature compares the number of errors to the threshold settings. By enabling this feature, you can log errors in the event log and shutdown the port that is receiving CRC error packets. Currently you can enable this feature only by using the CLI and only for ports on 50-series and 80-series gigabit modules. For more information about this feature, see "Network Error Detection and Recovery" in Chapter 5.

If NEDR shuts down a port, the switch will forward traffic through a redundant port if you:

- Enable a protocol that supports redundancy, such as OSPF, VRRP, or STP, on the port
- Provide an alternate path

If you do not enable a protocol that supports redundancy on the port and provide an alternate path, you may lose traffic if the port shuts down.

*** Note:** You can enable NEDR only for ports on gigabit Ethernet modules and only by using CLI commands. You cannot enable the feature on any other types of ports, for example, Ethernet 10/100, ATM Uplink, or supervisor, and cannot enable the feature by using the Web Agent.

*** Note:** If the switch has an 80-series supervisor module installed, monitoring begins as soon as you turn on the switch. If the switch has a layer 3 supervisor module installed, monitoring may not begin until approximately 35 seconds after you turn on the switch.

If the rate of CRC errors equals or exceeds the threshold value, the NEDR feature can:

- Disable the port

*** Note:** You can reenable the turned off port by entering the following CLI command:

```
set port enable
```

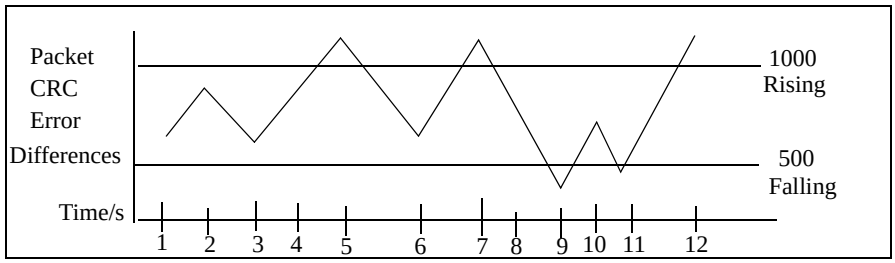
NEDR does not check for an available redundant port or for a redundant protocol running on the port. You must create a redundant path. Traffic loss will occur if a redundant path is not available.

- Log the event in the Event Log

If you replace a module that has a port that has been disabled by NEDR, the switch will load the startup configuration for the module and reenable the port. However, if you save the running configuration to the startup configuration while a port is shut down, you will have to manually reenable the port after you replace the module or reset the switch.

## Example

***Figure 6-10. Example of How NEDR Works***




In 6-10, the rising threshold is set to 1000, and the falling threshold is set to 500. The first time that the rate of CRC errors exceeds the rising threshold, NEDR logs the event in the event log or disables the port. If you set the feature to **notify**, NEDR does not log another event until the rate of CRC errors drops below the falling threshold and then exceeds the rising threshold again. If you set NEDR to **disable-port**, the feature disables the port the first time that the rate of CRC errors exceeds the rising threshold. The port remains disabled until you reenable it, or until you remove and replace/ reinsert a module of the exact type.

# Enabling NEDR

You can enable NEDR only on Gigabit Ethernet ports and only by using CLI commands.

To enable NEDR:

1. Enter Global Configuration mode.

   The CLI displays the `<configure>#` prompt.

   *** Note:** For information on how to enter this mode, see "Accessing/Exiting the Command Modes" in Chapter 1, "Overview," of *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3*.

2. Enter the following command:

   <configure># **set port network-error-detection {<mod-port-range> | <all>} [action {notify | disable-port | off}] [rising-threshold <rising-threshold-value>] [falling-threshold <falling-threshold-value>] [interval <interval-seconds>]**

Table 6-2 explains the keywords, arguments, and options for the **set port network-error-detection** command:.

***Table 6-2. set port network-error-detection Keywords, Arguments, and Options***

| Keywords, Arguments and Options | Explanation |
|---|---|
| <*mod/port-range*> | The slot number of the module, and, either port number, or range of port numbers. Enter the port ranges in the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**. |
| all | Disables NEDR on all ports on all modules in the switch. **all** can be used only with **off**. |
| | ***1 of 2*** |

***Table 6-2. set port network-error-detection Keywords, Arguments, and Options***

| Keywords, Arguments and Options | Explanation |
|---|---|
| action {notify \| disable-port \| off} | Action that NEDR performs when the rate of errors exceeds the threshold. The options are:<br>**notify** - Logs the event in the event log<br>**disable-port** - Disables the port and logs the event in the event log.<br>**Note:** A port will be disabled if the rate of errors equals or exceeds the threshold. Make sure a redundant protocol is configured.<br>**off** - Disables NEDR on the port or ports that you specify.<br>The default setting is **notify**. |
| <*rising-threshold value*> | The rising threshold.<br>The number of CRC errors that triggers NEDR to log an event in the event log or disable the port. The default setting is 100 (minimum is 1; maximum is 65535). |
| <*falling-threshold value*> | The falling threshold.<br>After exceeding the rising threshold, NEDR does not log another event in the event log until the rate of CRC errors falls below the falling threshold and then exceeds the rising threshold again. The default setting is half the rising threshold value (minimum is 0; maximum is 65535). |
| <*interval-seconds*> | How often NEDR checks the number of errors occurring against the thresholds. Enter a number of seconds.<br>The default setting is 2 seconds (minimum is 1; maximum is 65535). |
| | ***2 of 2*** |

*** Note:** If you set the rising threshold value and the falling threshold value close together, events may be logged more often if the **Notify** option is selected.

The CLI displays a confirmation message if you successfully enable NEDR for a port or range of ports.

If no message displays, the port information was invalid. To verify that NEDR is enabled on a port, enter the following CLI command:

```
<configure># show port network-error-
detection
```

If the port is not listed as enabled for NEDR, reenable NEDR on the same port or ports again.

*** Note:** There is no Configuration Event for enabling or disabling NEDR in the Event Log. However, you can find out which ports have NEDR enabled using the following CLI command:

>**show port network-error-detection**

# Internal Error Detection and Recovery

## Overview

Version 5.3.1 contains the Internal Error Detection and Recovery (IEDR) feature. This feature shuts down a port if its rate of internal errors exceeds the threshold setting. Currently you can enable this feature only by using the CLI and only for ports on 50-series and 80-series Gigabit Ethernet modules. By default IEDR is disabled.

This feature is designed to serve as mechanism for detecting and isolating hardware failures.

If IEDR shuts down a port, the switch will forward traffic through a redundant port if you:

- Enable a protocol that supports redundancy, such as OSPF, VRRP, or STP, on the port
- Provide an alternate path

If you do not enable a protocol that supports redundancy on the port and provide an alternate path, you may lose traffic if the port shuts down.

If you replace a module that has a port which has been disabled by IEDR, the switch will load the startup configuration for the module and reenable the port. However, if you save the running configuration to the startup configuration while a port is shut down, you will have to manually reenable the port after you replace the module or reset the switch.

## Enabling IEDR

*** Note:** To enable IEDR for ports in a hunt group, you must use a different command that enables the feature globally for all ports in all hunt groups on the switch. For information on this command, see "Enabling IEDR for Hunt Groups" on page 5-45.

*** Note:** **(SPR 5938)** Do not use ISL Tagging (Trunk Mode: Multilayer) on ports that have IEDR enabled.

IEDR is disabled by default on gigabit ports. To enable the feature:

1. Enter Global Configuration mode.

   The CLI displays the `<configure>#` prompt.

   *** Note:** For information on how to enter this mode, see "Accessing/Exiting the Command Modes" in Chapter 1, "Overview," of *Cajun P550R/P880/P882 Command Line Interface Reference Guide*.

2. Enter the following command:

   **set port internal-error-shutdown {<slot>/<port> | <slot> | all-ports} enable**

To disable IEDR, enter:

**set port internal-error-shutdown {<slot>/<port> | <slot> | all-ports} disable**

## Enabling IEDR for Hunt Groups

This procedure globally enables IEDR for all ports in all hunt groups on the switch.

*** Note:** **(SPR 5909)** All ports that are enabled for IEDR will be subjected to the hunt group IEDR setting if they are placed in a hunt group whether they are administratively disabled or enabled. Ports that are enabled for IEDR before being placed in a hunt group will still display when showing configuration but they still will be subjected to take on the hunt group setting until they are removed from the hunt group.

To globally enable IEDR for all ports in hunt groups:

1. Enter Global Configuration mode.

   The CLI displays the <configure># prompt.

2. Enter the following command:

   **set huntgroup internal-error-shutdown enable**

To globally disable IEDR for all ports in hunt groups, enter:

**set huntgroup internal-error-shutdown disable**

## Setting the IEDR Threshold for Internal Errors

You can set the threshold at which the switch will shutdown a port. By default this threshold is set to 10 internal errors in a 5-second time period. You can set the threshold to any number between 5 and 500 internal errors in a 5-second time period. This setting is global for all ports that have been enabled for IEDR including ports configured for Hunt groups.

To set the IEDR threshold:

1. Enter Global Configuration mode.

   The CLI displays the <configure># prompt.

2. Enter the following command:

   **set internal-error-threshold <*threshold*>**

## Viewing IEDR Settings

To view a list of the ports that have IEDR enabled:

1. Enter Global Configuration mode.

   The CLI displays the <configure># prompt.

2. Enter the following command:

   **show port internal-error-config**

## Viewing IEDR Settings for Hunt Groups

To view the global IEDR setting for hunt groups:

1. Enter Global Configuration mode.

   The CLI displays the <configure># prompt.

2. Enter the following command:

   **show hunt group internal-error-config**

## Error Messages

*** Note:** If IEDR detects errors on a port in the huntgroup, it tests each port within that hunt group. When it finds the first bad port, it removes it from the Hunt Group and disables the port.

The IEDR feature may display the following error messages:

- The following message indicates the IEDR feature is enabled on the specified ports

  — `internal-error-config enabled on port <x>/<y>`

- The following message indicates that internal CRC errors are occurring:

  — `Description: CRC err: Rx'ed 5 bad pkts since last poll - last from port3.2`

- The following message indicates that IEDR shut down a port because its rate of internal errors exceeded the threshold:

  — `Description: Shutdown Port 3.2 due to CRC error exceeding threshold of 10`

## System Messages

The **set port internal-error-shutdown all-ports enable** command produces system messages similar to the following:

- Upon success:

```
Internal-error-config enabled on port 3/1
Internal-error-config enabled on port 3/2
Internal-error-config enabled on port 4/1
Internal-error-config enabled on port 4/2
Internal-error-config enabled on port 4/3
Internal-error-config enabled on port 4/4
```

```
Slot 6 has 10/100 ethernet ports that are
unsupported and will not be set.
```

*** Note:** IEDR is only supported for 50 and 80 series Gigabit modules.

```
Internal-error-config enabled on port 7/1
Internal-error-config enabled on port 7/2
Internal-error-config enabled on port 7/3
Internal-error-config enabled on port 7/4

Feature enabled for port(s) specified

If CRC Error Threshold is exceeded then port
will automatically be shut down.

TRAFFIC LOSS WILL RESULT if no redundant port
is configured and port shutdown occurs.

To UNDO use: "set port internal-error-
shutdown {slot/port} disable"
```

- Upon Failure:

The **set port internal-error-shutdown all-ports disable** command produces system messages similar to the following:

- Upon Success:

```
Internal-error-config disabled on port 3/1
Internal-error-config disabled on port 3/2
Internal-error-config disabled on port 4/1
Internal-error-config disabled on port 4/2
Internal-error-config disabled on port 4/3
Internal-error-config disabled on port 4/4

Slot 6 has 10/100 ethernet ports that are
unsupported and will not be set.

Internal-error-config disabled on port 7/1
Internal-error-config disabled on port 7/2
Internal-error-config disabled on port 7/3
Internal-error-config disabled on port 7/4

Feature disabled for port(s) specified

Port(s) will not be shut down if CRC Threshold
Exceeded.
```

- Upon Failure:

```
Don't Shutdown all ports failed
```

The **set internal-error-threshold <*5-500*>** command produces system messages similar to the following:

- Upon Success:

  ```
  Threshold value set to 10
  ```

- Upon Failure (The only failure that can occur is that the number entered was not in the range 5 – 500):

  ```
  Threshold value must be between 5 and 500
  ```

# 6 Managing the Address Forwarding Table

## Overview

The Address Forwarding Table (AFT) is a mapping table of MAC addresses with their associated port locations.The AFT is used by the Avaya Multiservice switch to correctly forward (bridge) frames destined for a particular MAC address to the correct physical port. The AFT performs several major functions, learning new MAC addresses, aging out old MAC addresses, and providing a management interface to display, add, modify, and remove AFT entries (MAC addresses). AFT's are maintained throughout the system, on media modules and the supervisor module.

There is one AFT created for each VLAN. The entire Avaya Multiservice Switch can store up to 24,000 MAC addresses and 1000 VLANs.

*** Note:** Although the Avaya Multiservice Switch can support 1000 VLANs, (in Fabric mode 2 with all 80 series modules), restrictions apply for the size of the Hash tables, the size of the Address Forwarding Tables and the number of VLANs. This information is detailed in the following pages in this chapter.

- New address Learning - When a MAC address of a packet is unknown, it must be learned by the AFT
- Address Aging - On a periodic basis (which is configurable) the addresses in the AFT are aged out, MAC addresses not received for a period of time (e.g. 5 minutes) are removed from the AFT along with their port associations.
- Static Address Management - Static MAC address entries are saved in memory upon module reset. These static address always exists in the AFT, and are not aged out or overwritten.Static entries are those manually configured. Each VLAN and its AFT has 18 AFT entries automatically entered by the switch that are reserved for internal use.
- Address Management - The user has the ability to display entries, add entries to the AFT, remove entries from the AFT, and change entries within the AFT. This is accomplished

through the Web Agent interface or CLI commands. A user can also make an entry or entries static, which saves the entries upon module reset.

## Chapter contents

The following information and procedures are in this chapter.


- Relationship between VLANs, AFT and Hash Table Sizes
- Configuring Hash table and AFT parameters
- Configuring the AFT
- Searching the AFT
- Adding Entries to the AFT Manually


# Relationship between VLANs, AFT and Hash Table Sizes

## Hash Tables and Buckets

For every VLAN created, a hash table is allocated. The hash table keeps track of the memory locations where the learned AFT entries (MAC addresses) are stored. These memory locations are referred to as *buckets*.

An individual *bucket* can range in size from 1 to 128 AFT entries (MAC addresses) in powers of 2 (1, 2, 4, 8, 16...). The *bucket capacity* for a VLAN is the sum of all the capacities of the *buckets* assigned to that VLAN. If you add the number of Address Forwarding Table (AFT) Entries and divide by the *Bucket Capacity*, you will get the percentage of *Bucket Utilization* (Figure 6-1).

To view the *Bucket* parameters from the Web Agent, expand the **Layer 2 Switching** > **Address Forwarding Table** > **Configuration** folders. And view the **Bucket Capacity** and **Bucket Utilization** fields.

## Hash Table and Bucket memory usage guidelines

The Avaya Multiservice switch provides 60K of memory that is used to store hash tables and AFT buckets. In general, no more then 20K should be used for Hash Tables, leaving 40K available for AFT entries (MAC addresses). It is important to take into consideration the number of VLANs that the switch will have when determining the hash table size for each VLAN, as the total amount of memory used for the Hash Tables should not exceed 20K. As more VLANs are created, the smaller each VLANs Hash Table should be.

It is not advised to allow the total hash table memory usage to exceed 20K. More than 20K will limit the potential for growth (i.e., address learning). If your Avaya Multiservice switch is approaching this threshold, adjust the Initial Hash Table Size accordingly.

For example, if you anticipate creating more than 20-30 VLANs, the Initial Hash Table Size default setting must be reduced. The rule of thumb is the following formula:

Number of VLANs *times* Initial Hash Table Size <20K

Example 1: 30 x 512 ~ 15K

Example 2: 1000 x 16 ~ 16K

*** Note:** When you create a VLAN, there are 18 internal MAC entries automatically created for that VLAN. If you were to configure Example 2, the switch would indicate that 36K of memory is currently in use. This is because you have 16K of memory for the VLAN Hash Tables and another 20K of memory used for the 18,000 MAC entries.

# Hash Table guidelines for creating VLANs

## Maximum Number of VLANs

In order to support the maximum number of VLANs, VLAN ID numbers should be chosen from the range of 1 to 1000. The numbering of VLANs has no impact on memory usage within the switch. The numbering of VLANs only effects the total number of supported VLANs. This is not a memory usage issue, however, it does effect the way the switch uses or Hashes VLAN ID's. If VLAN ID's are used outside of the range of 1 to 1000, there is a possibility of unavailable VLAN ID's. This again does not effect switch memory usage. If VLANs are already created with VLAN ID's outside of the 1-1000 range, there is no need to reassign new VLAN ID's. The only potential issue could be particular VLAN ID's might not be available.

## VLAN ID number outside the recommended range

If you use an ID number outside the range of recommended numbers, you may find certain VLAN ID numbers cause "collisions" and are unavailable when you try to create a new VLAN.
The reason for this has to do with the way that the switch hashes VLAN numbers into internal tables. The 'hash' algorithm used by the switch takes VLAN numbers (which have a range from 1 to 4094) and 'hashes' them to a range of 1 to 1024 by picking 10 bits from the VLAN number. This smaller range is used as an index into

tables within the switch, and will be referred to as the ‘index’. Because the algorithm maps 4096 VLAN numbers to 1024 indexes, it is easy to see that more then one VLAN number may map to the same index. This is known as a ‘hash collision’.
When a collision occurs, the switch attempts to resolve the hash collision by using 10 other bits from the VLAN ID. When the switch cannot find 10 bits that uniquely hash the VLAN number, an error is returned to the user that the VLAN number cannot be added. In order to avoid this situation, it is suggested that the user pick VLAN numbers only from the range of 1 to 1000, as when this is the case, it is guaranteed that the switch can hash this set of VLAN numbers without having any collisions that cannot be resolved. Specifically, the 10 least significant bits are picked, which hash each VLAN number (in the range of 1 to 1000) to an index that is the same as the VLAN number. In this situation there will never be any collisions. See the Maximum Number of VLANs Supported section for valid ranges.

## Reassign VLAN IDs?

It is not recommended to reassign VLAN numbers in a switch that is currently using VLAN numbers outside the range of 1 to 1000. The only potential issue is an attempt to add more VLANs, it is possible that particular VLAN numbers will not be available to use.

## Optimal Bucket Utilization and Hash Table size

To achieve optimal Bucket Utilization, Hash Table size should be ¼ times the number of expected AFT entries (MAC entries) on the VLAN.

*** Note:** Each VLAN has 18 AFT entries automatically entered by the switch that are reserved for internal use. (Refer to Chapter 1, *“Introduction”*, of the *Avaya P550R, P580, P880, and P882 Multiservice Switch User Guide, Version v5.3.1* for detailed listing of Self Addresses).The total amount of AFT memory used for Hash Tables should not exceed 20K.

## Maximum Number of VLANs

The following information provides the maximum number of VLANs that are supported depending on the version of code that is running and the "Fabric Mode" that the switch is configured with.

*** Note:** Pre-5.0 code does not support 'fabric modes', and when a switch is in Fabric Mode 2, only Cajun II hardware is supported.

If the number of VLANs supported in the switch is 500, then the VLAN ID numbers used in the switch should be chosen from the range of 1 to 500 rather then 1 to 1000.

***Table 6-3. Number of Supported VLANs***

| Version of Code | Fabric Mode 1 | Fabric Mode 2 |
|---|---|---|
| **Pre-5.0** | **1000** | **N/A** |
| **5.0-Pre 5.2.10** | **500** | **500** |
| **5.2.10 and above** | **500** | **1000** |

Table 6-2 is an example of the size of the hash table created per the number of VLANs created using the guidelines.

***Table 6-4. Number of VLANs and Hash Table Size:***

| Number of VLANs | Hash Table Size |
|---|---|
| 2 | 8192 |
| 4 | 4096 |
| 10 | 2048 |
| 20 | 1024 |
| 40 | 512 |
| 80 | 256 |
| 150 | 128 |
| 300 | 64 |
| 600 | 32 |
| 1000 | 16 |

# Examples of Configuring VLANs and Hash Table Size

## Example 1

**All VLANs have the *same* Hash Table Size**

Configure the Avaya Multiservice switch for 45 VLANs.This requires the default Hash Table size be reduced in accordance with the “Hash Table Guidelines”.

45 VLANs *times* 1024 = 46,080 or ~ 46K

This exceeds the 20K guideline for the amount of AFT memory used for Hash Tables. Even if the Hash Table size is reduced by half, it still exceed the guideline. In order to comply with the guideline, the Initial Hash Table Size for each VLAN should be 256 or less. 45 VLANs *times* 256 = 11,520 or ~ 12K This leaves 48K for AFT entries (60K - 12K = 48K).

## Example 2

**VLANs have the *different* Hash Table Sizes**

Configuring the Avaya Multiservice switch for 6 “large” VLANs (4000 users on each), 30 “medium” VLANs (1000 users on each), and 50 “small” VLANs (200 users on each). Using the “Hash Table Guidelines”, each “large” VLAN should have a hash table size around (1/4)*4000=1000, each “medium” VLAN around (1/4)*1000=250, and each “small” VLAN should have a hash table size around (1/4)*200=50. We also want to make sure that the total amount of memory used for the Hash Tables is less then 20k, which it will be (~17K).

6 VLANs *times* 1024 = 6,144

30 VLANs *times* 256 = 7,680

50 VLANs *times* 64 = 3,200

Total AFT Memory used or Hash Tables = 17,024 or ~ 17K

This meets the guideline.

# AFT Default Settings

*Figure 6-11. Create VLANs*

**Hash Table Size Default Settings (refer to figure 6-1)**
**Name** - Name for the new VLAN

**ID** - VLAN ID number, valid number between 1-4094 (1 is reserved for the Default VLAN)

**Instance ID** - Instance table representation of a VLAN. The Instance ID does not directly correlate to the VLAN ID

**Hash Table Size** - 1024, the default setting for the Initial Hash table size.
**Auto- Increment HT Size** - Default setting is *True*. Enable to automatically correct for undersized hash table size.

# Address Forwarding Table, Auto-Sizing, Auto Increment and Threshold

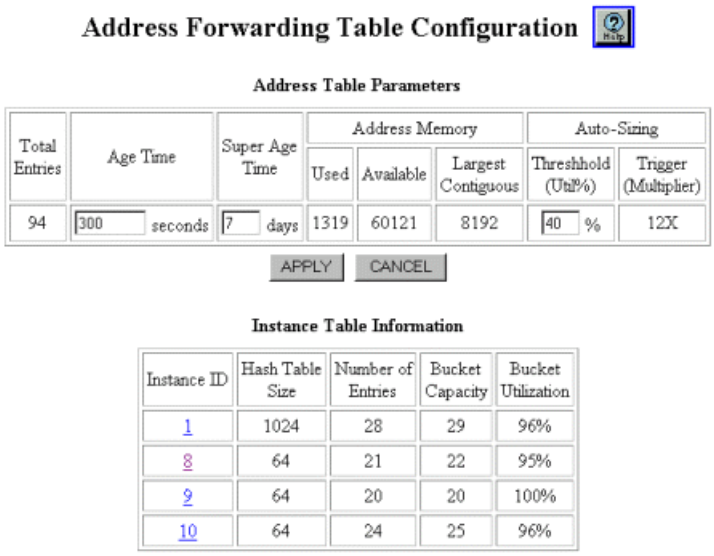
## Default Settings

Select **Configuration** from the **L2 Switching** > **Address Forwarding Table** group in the Web Agent window. The **Address Forwarding Table Configuration** dialog box opens (Figure 6-12)

*Auto-Sizing* is a feature that allows the Avaya Multiservice Switch to automatically correct for an undersized hash table, which can result in poor AFT memory utilization. Auto-Sizing consists of three

parameters: *Auto-Increment*, *Trigger* (Multiplier), and *Threshold* (Util%) in the Address Forwarding Table Configuration

***Figure 6-12. Address Forwarding Table Configuration***




## Auto-Increment

*Auto-Increment* is the Enable/Disable setting for the Auto-Sizing feature. If Auto-Increment is enabled, the switch will automatically increase the hash table size provided two conditions are met.Refer to figure 6-1 for enabling or disabling Auto-Increment HT size.

## Trigger (Multiplier)

The first condition is the *Trigger (Multiplier)*, which sets a minimum threshold for the number of learned entries a VLAN must have before the switch will consider increasing the Hash Table size. This prevents the Avaya Multiservice Switch from resizing Hash Tables for VLANs who have only a few AFT entries. This threshold is 12 times the Hash Table size.

For Example: If a VLAN is created with an Initial Hash Table Size of 64, the trigger would be 12 *times* 64 = 768 learned entries. If there are more than 768 learned entries, the second condition is evaluated.

## Threshold (Util%)

The second condition is met if Bucket Utilization drops below the *Threshold (Util%)*, which by default is 40%. The switch will compensate for the poor utilization by doubling the Hash Table. 40% is recommended for most applications.

Resizing results in the switch utilizing AFT memory more efficiently. When the switch resizes the Hash Table, all entries are flushed and must be relearned.

**It is highly recommended the default of 40% not be changed. The affects of varying the Threshold (Util%) are as follows:**

- *Increasing* Threshold: Gives better memory utilization at the expense of more frequent flushing, flooding, and relearning.
- *Decreasing* Threshold: Gives less efficient memory utilization but does not flush, flood and relearn as often.

# Total Entries, Address Memory, Age and Super-Age Timers

## Overview

You can see the Total Entries and Address Memory. You can configure address age, auto-sizing threshold, and Super Age timers. Refer to Figure 6-2.

### Total Entries

Display how many address entries are contained in the table.

### Address Memory

Displays how much address memory is currently being used, the amount of memory still available, and the largest contiguous block of memory that can exist.

### Address Age and Super Age timers

- **Address Age Time -** defines the length of time addresses remain active in the address forwarding table.
- **Super Age Time** - defines how long inactive addresses are stored in the address forwarding table before being deleted.

## Configuring the AGE and Super Age Timers

### Web Agent Procedure

You can configure the Age Timer and Super Age Timer by using either the Web Agent or the CLI.

Enter a value in the **Age Time** field. Aged out addresses become invalid until the switch sees another packet with the aged out entry's source address.The standards-recommended default is 300 seconds.

*** Note:** If you have ATM Uplink Modules in the chassis and you set the **Age Timer** value to less than 30 seconds, you must change the **Flush MAC Timer** on each ATM Uplink module to be less than or equal to the new **Age Timer** value.

Enter a new value in the **Super Age Time** field. The valid entries are 1-30 days. The Super Age Timer marks all invalid table entries, then checks to see if they remain invalid for the specified super age interval. This clears the table of entries that are no longer used. The default value is 7 days.

Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### CLI Commands

To change the aging values for all instances of the Address Forwarding Table from the CLI, enter one of the following commands from **Configure** mode:

```
<configure># set aft agetime <age-time-value>
<configure># set aft super-agetime <age-time-
value>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Instance Table Information

The Instance Table Information, is a summary of a AFT instance or Hash Table settings and utilization per VLAN. Refer to Figure 6-2.

### Instance ID, Hash Table Size, Number of Entries, Bucket Capacity, and Bucket Utilization

**Instance ID** - Individual AFT Hash Table settings and utilization, each ID would correlate to a VLAN.

**Hash Table Size** - Memory space available for the Hash Table per Instance or VLAN

**Number of Entries** = The Total Number of Entries (MAC Addresses) for that VLAN

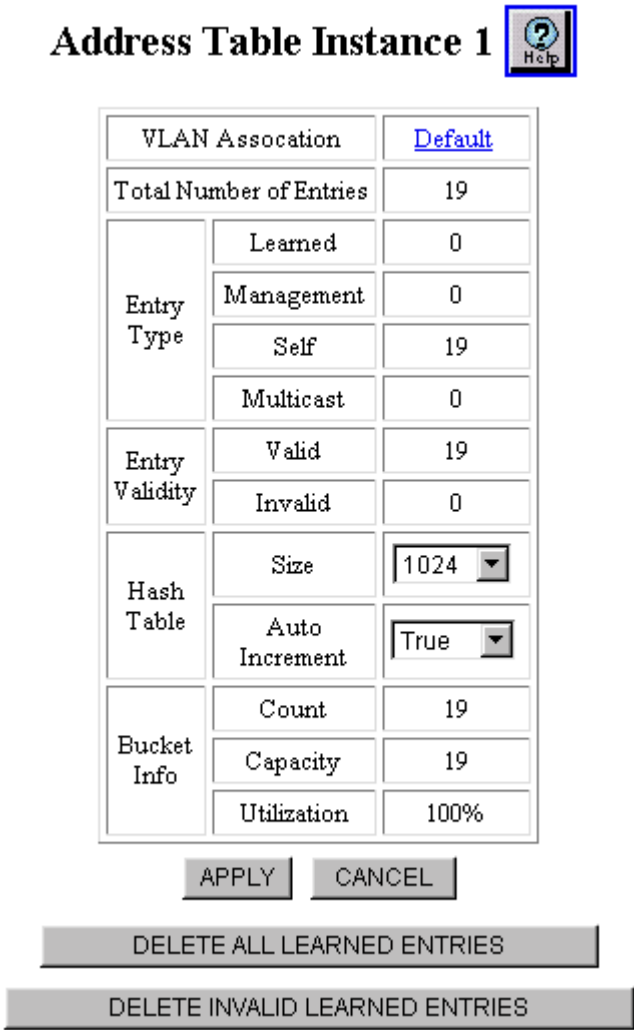
**Bucket Capacity** = The bucket capacity for a VLAN is the sum of all the capacities of the buckets assigned to that VLAN.

**Bucket Utilization** = The number of entries divided by the Total Bucket Capacity times 100 =% of utilization.

## Instance Table

Click the ***ID*** number in the ***Instance IDs*** column, to achieve finer control of a particular VLAN table. The ***Address Table Instance*** screen displays for the instance ID selected.(Refer to Figure 6-13)

*Figure 6-13. Address Table Instance Dialog Box*




Refer to Table 6-5 for a definition of the Address Table Instance dialog box parameters.

*Table 6-5. Address Table Instance Parameters*

| Parameter | Definition |
|---|---|
| **VLAN Association** | Name of the VLAN this Hash table is associated with. |
| **Total Number of Entries** | Displays the total number of entries (MAC addresses) for this VLAN. |
| **Entry Type** | Displays the entry type for this VLAN.<br>Options include:<br>• **Learned** - Entry is dynamically learned.<br>• **Management** - Entry is configured by the user statically.<br>• **Self** - Entries for internal addresses contained within the switch.<br>• **Multicast** - Entries belong to Multicast Groups. |
| **Entry Validity** | Displays the entry validity for this VLAN.<br>Options include:<br>• **Valid** - Entry exists.<br>• **Invalid** - Entry has aged out but still exists even though the port binding is invalid. |
| | ***1 of 2*** |

*Table 6-5. Address Table Instance Parameters*

| Parameter | Definition |
|---|---|
| **Hash Table** | Select one of the following hash table parameters:<br>Size - Select the size to alter the space available for this address table. The selection range is 16 to 8192 incrementing in the powers of 2.<br>**Note:** The number of addresses for a given hash table is 4:1 (for example, if you have a hash table of 16 bytes, the VLAN can hold 64 addresses in it's table instance.To achieve optimal Bucket Utilization, Hash Table size should be ¼ times the number of expected AFT entries (MAC entries) on the VLAN.<br>**Auto Increment** - Select an option to allow the hash table to grow dynamically larger if more addresses are discovered. The options are:<br>**True** - Enables auto-increment of the hash table.<br>**False** - Disables auto-increment to prevent the hash table from growing dynamically at the risk of extra flooding. |
| **Bucket Info** | Displays parameters to monitor the efficiency of the hash table allocations.<br>Options include:<br>• **Count** - The Total Number of Entries (MAC Addresses) for that VLAN<br>• **Capacity** - Indicates bucket capacity.<br>• **Utilization** - The number of entries divided by the total bucket capacity. |
| | ***2 of 2*** |

**3.** Click:

- **APPLY** to save your changes
- **CANCEL** to restore previous settings
- **Delete All Learned Entries** if you want to relearn the entire table
- **Delete Invalid Learned Entries** if you want to delete all entries that are currently aged out.

*** Note:** If you change the Hash Table Size, the switch relearns all addresses in that table, causing the switch to flood packets for a few seconds.

### Controlling Reconfiguration of AFT Sizes Using the Web Agent

To manually control reconfiguration of AFT sizes using the Web Agent:

1. Select **Configuration** from the **L2 Switching** > **Address Forwarding Table** group in the Web Agent window. The **Address Forwarding Table Configuration** dialog box opens (Figure 6-12).

2. Enter a new **Auto-Sizing Utilization Threshold** percentage in the Threshold (Util%) field, if you just want to cause the table reconfiguration to occur at a different level of usage efficiency. The default value of 40% is recommended for most applications.

   *** Note:** Raising the value in the Threshold (Util%) field might cause the table to be relearned more frequently, and makes address space usage more efficient.

### Controlling Reconfiguration of AFT Sizes Using the CLI

To manually control reconfiguration of AFT sizes using the CLI, enter the following command in **Enable/Configure** mode:

```
<configure># set aft auto-sizing-threshold
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Searching the Switch AFT

The AFT can hold 24,000 entries on each switch. The switch Web Agent provides a utility that allows you to filter which addresses it displays, making the list more manageable. Multiple criteria can be selected to produce a sophisticated filter. The parameters are treated as “ands,” meaning that displayed addresses must meet all selected criteria.

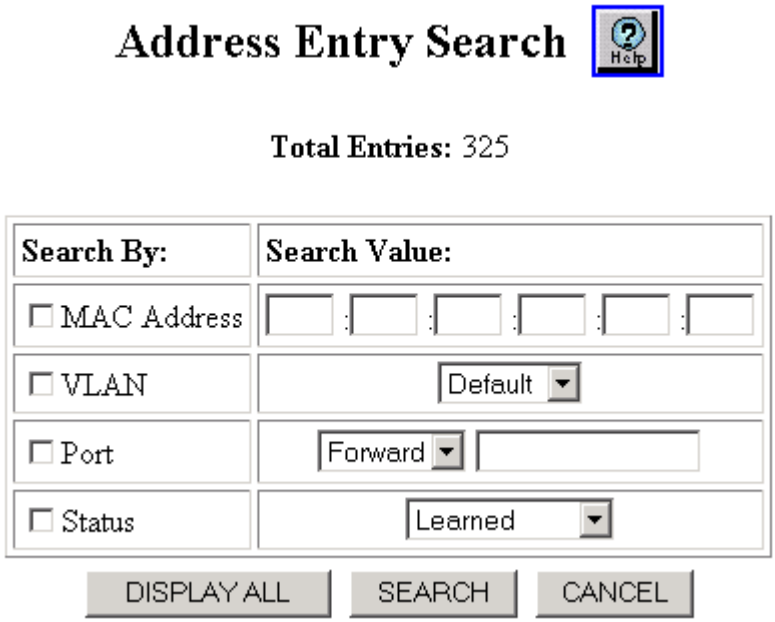
You can search the AFT using the Web Agent or the CLI.

### Searching the Switch AFT Using the Web Agent

To filter the AFT using the Web Agent:

1. Select **Address Search** from the **Address Forwarding Table** group on the Web Agent window. The **Address Entry Search** dialog box opens (Figure 6-4)

*Figure 6-14. Address Entry Search Dialog Box.*




*** Note:** "DISPLAY ALL" ignores any parameter not checked in the left column. To view all addresses in the table, select "DISPLAY ALL" without selecting any filters.

2. To search using a MAC Address:
   - Select the MAC Address checkbox in the **Search By:** column
   - **Enter a MAC address in the** Search Value column.

   *** Note:** You must enter the complete MAC address.

3. To search using a VLAN:
   - Select the VLAN checkbox in the **Search By:** column
   - Select a VLAN name from the **VLAN** field pull-down menu in the **Search Value:** column.

4. To search using a Port:
   - Select the Port checkbox in the **Search By:** column
   - Select a search variable from the Port field pull-down menu. The options are: Forward, Filter, and CPU

— Enter a port number to display only the entries associated with that switch port.

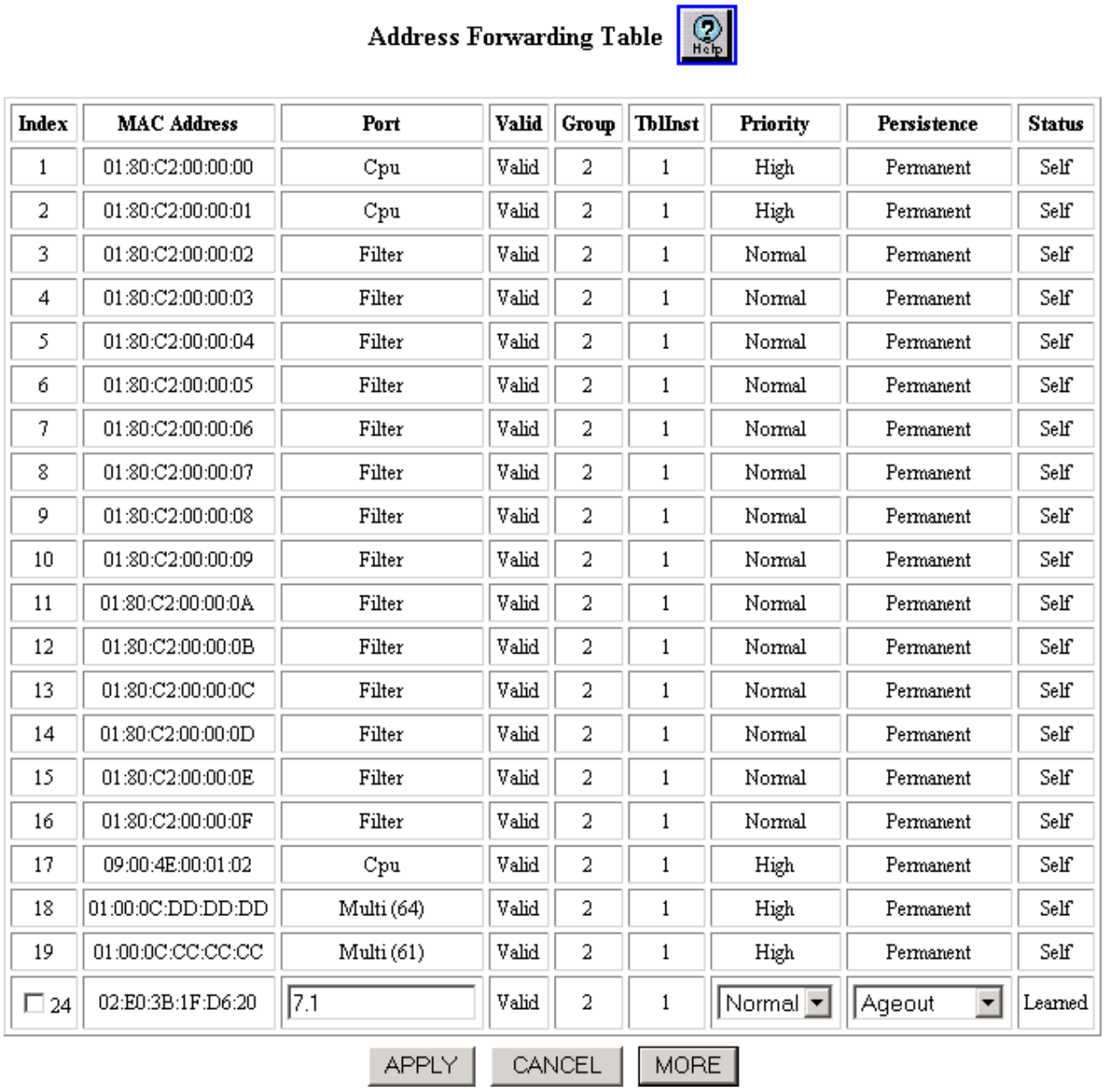
5. To search using a bridging status:

— Select the **Status** checkbox in the **Search By:** column

— Select a status from the pull-down menu to show only ports of a specific bridging status. The options are: Learned, Management, Self, and Multicast.

6. Select **DISPLAY ALL** to open the **Address Forwarding Table** dialog box (Figure 6-4).

*Figure 6-15. Address Forwarding Table Dialog Box*



Address Forwarding Table

| Index | MAC Address | Port | Valid | Group | TblInst | Priority | Persistence | Status |
|---|---|---|---|---|---|---|---|---|
| 1 | 01:80:C2:00:00:00 | Cpu | Valid | 2 | 1 | High | Permanent | Self |
| 2 | 01:80:C2:00:00:01 | Cpu | Valid | 2 | 1 | High | Permanent | Self |
| 3 | 01:80:C2:00:00:02 | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 4 | 01:80:C2:00:00:03 | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 5 | 01:80:C2:00:00:04 | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 6 | 01:80:C2:00:00:05 | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 7 | 01:80:C2:00:00:06 | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 8 | 01:80:C2:00:00:07 | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 9 | 01:80:C2:00:00:08 | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 10 | 01:80:C2:00:00:09 | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 11 | 01:80:C2:00:00:0A | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 12 | 01:80:C2:00:00:0B | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 13 | 01:80:C2:00:00:0C | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 14 | 01:80:C2:00:00:0D | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 15 | 01:80:C2:00:00:0E | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 16 | 01:80:C2:00:00:0F | Filter | Valid | 2 | 1 | Normal | Permanent | Self |
| 17 | 09:00:4E:00:01:02 | Cpu | Valid | 2 | 1 | High | Permanent | Self |
| 18 | 01:00:0C:DD:DD:DD | Multi (64) | Valid | 2 | 1 | High | Permanent | Self |
| 19 | 01:00:0C:CC:CC:CC | Multi (61) | Valid | 2 | 1 | High | Permanent | Self |
| 24 | 02:E0:3B:1F:D6:20 | 7.1 | Valid | 2 | 1 | Normal | Ageout | Learned |

APPLY CANCEL MORE

*** Note:** Some types of entries in the Address Forwarding Table can be modified. The port, priority, and persistence can be changed for learned and management entries.

7. To change an entry in the Address Forwarding Table, select the checkbox in the Index column for MAC address entry.

8. Make the change(s) to the port, priority, or Persistence for the selected entry

9. After making the changes, click the **APPLY** button to save the current settings, or **CANCEL** to restore previous settings. or **MORE** to view more statistics.

10. Refer to Table 6-6 to review your search criteria options:

***Table 6-6. Address Forwarding Table Parameters***

| Parameter | Defines the... |
|---|---|
| **Index** | Index number of this address entry in the switch address forwarding table. |
| **MAC Address** | MAC address associated with this entry. This address is learned by the switch as an address to forward to the associated port. |
| **Port** | Port associated with this MAC address table entry. |
| **Valid** | An entry is valid until it ages out, at which time it becomes invalid. Aging out occurs when a frame with the entry's MAC address is not received during the address age time interval. An invalid entry can become a valid entry again if the entry's MAC address is learned (frame is received) during the super age time interval. If the super age time interval expires before the MAC address is learned again, the entry is deleted." |
| **Group** | Group number associated with this MAC address. |
| **TblInst** | Address table instance number associated with this MAC address. |
| **Priority** | Priority level associated with traffic forwarded to this MAC address. The options are:<br>• **Normal**<br>• **High**<br>You can set this parameter on all learned entries. |

*Table 6-6. Address Forwarding Table Parameters continued*

| Parameter | Defines the... |
|---|---|
| **Persistence** | The persistence of the entry in the table can be set on all learned entries:<br>• **Permanent -** The address is not aged out of the table.<br>• **Invalid -** This entry is cleared from the table each time the switch resets.<br>• **Ageout -** Address is cleared from the address forwarding table when the timeout interval expires. This is the state of all entries dynamically learned by the switch. It ensures that MAC addresses that are not active on the network do not remain in the switch address forwarding table indefinitely.<br>**Note:** If you create a static, filtered MAC address and set **Persistence** to **Ageout**, the switch does not filter the MAC address. The switch continues to forward frames that have the MAC address for a source address or destination address. To correct this, set Persistence to Permanent. |
| **Status** | The status of the address entry.<br>Options include:<br>• Learned<br>• Management<br>• Self AFT Self Entries:<br>• 01:80:C2:00:00:00 - 01:80:c2:00:00:0F - 802.1D reserved addresses, the first entry is the Spanning Tree BPDU destination address.<br>• 09:00:4E:00:01:02 - 3Com Vlan Trunk (VLT) control frame address. Used for Spanning Tree blocked ports that are in 3Com tagging mode and connected to a port on the other side of a connection that is blocked by Spanning Tree.<br>• 01:00:0C:CC:CC:CC - Cisco control frame. Used to synchronize VLAN membership across switches (VTPs) or router information between routers (CDPs). The switch sends them to the CPU, the CPU will set the BPDU bit when transmitting out a port trunking ISL.<br>• 01:00:0C:DD:DD:DD - If Cisco Group Management Protocol (CGMP) is enabled, the switch may listen to gather multicast group information |

### Searching the Switch AFT Using the CLI

To search the switch AFT using the CLI, enter the following command in **Configure** mode:

```
<configure># show aft entry
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Adding Entries to the AFT Manually

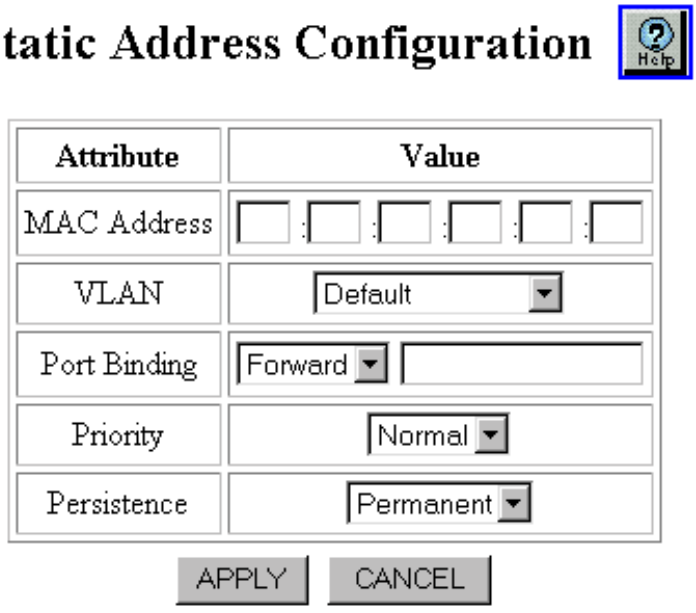
You can add entries to the AFT manually using the Web Agent or the CLI.

### Adding Entries to the AFT Manually Using the Web Agent

To add an AFT address manually using the Web Agent:

1. Select Entry Configuration from the Address Forwarding Table group in the Web Agent window. The Static Address Configuration dialog box opens (Figure 6-16).

***Figure 6-16. Static Address Configuration Dialog Box.***




2. Enter the MAC address that you want to add to the table in the MAC Address Value field.

3. Select a VLAN for this entry from the VLAN field pull-down menu.
4. Select Forward or Filter from the Port Binding field pull-down menu.If filter is selected, frames with the specific MAC address will be dropped.
5. Enter the port that you want associated with this entry in the Port Binding field.
6. Select a priority level from the Priority field pull-down menu for packets that you want forwarded to this MAC address. High priority addresses move to the front of the switch packet buffers automatically.
7. Select the persistence of Permanent or Ageout from the Persistence field pull-down menu.
8. Refer to Table 6-7 for an explanation of the Aging and Persistence field parameters:

***Table 6-7. Entry Persistence***

| Parameter | Definition |
|---|---|
| **Permanent** | The address is saved in nonvolatile memory and is not aged out of the table. |
| **Ageout** | Address is cleared from the address forwarding table when the timeout interval expires. This is the state of all entries dynamically learned by the switch. It ensures that MAC addresses that are not active on the network do not remain in the switch address forwarding table indefinitely. |

9. Click APPLY to save your changes, or CANCEL to clear the dialog box fields.

## Adding Entries to the AFT Manually Using the CLI

To add entries to the AFT manually using the CLI, enter the following command in Configure mode:

```
<configure># set aft entry (mac address)
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Option 82 for DHCP

Option 82 for DHCP includes two suboptions:

- Suboption 1 identifies the slot and physical port number from which the DHCP request was received.
- Suboption 2 identifies the IP address and, if available, the system name of the switch.

By default, both of these suboptions are enabled. You can change the status of either or both suboptions by using the Web Agent, Command Line Interface (CLI), or SNMP.

## Changing the Status of Option 82 by Using the Web Agent

To use the Web Agent to change the status of option 82:

1. Open the IP Global Configuration Web page.

   For information on how to open this Web page, see "Enabling IP Routing" in Chapter 9, "*Configuring IP Routing*," of the *Avaya P550R, P580, P880, and P882 Multiservice Switch User Guide, Version v5.3.1*.

2. Enable or disable the suboptions as appropriate in the **DHCP Option - Circuit Info** and **DHCP Option 82 - Agent Info** fields.

## Changing the Status of Option 82 by Using the CLI

To use the CLI to change the status of option 82, enter Global Configuration mode and use the following commands:

- To enable suboption 1, use the following command:

  **Avaya(configure)#ip dhcp circuit-info**

- To enable suboption 2, use the following command:

  **Avaya(configure)#ip dhcp agent-info**

- To disable suboption 1, use the following command:

  **Avaya(configure)#no ip dhcp circuit-info**

- To disable suboption 2, use the following command:

  **Avaya(configure)#no ip dhcp agent-info**

*** Note:** For information on how to enter Global Configuration command mode, see "Accessing/Exiting the Command Modes" in Chapter 1, "*Overview*," of the '"*Avaya P550R, P580, P880, P882 Multiservice Switch Command Line Interface Reference Guide, version 5.3.1*".

## Changing the Status of Option 82 by Using SNMP

To change the status of option 82 by using SNMP, use the MIB objects that are listed in Table 3. These MIB objects are located in **cjnipv4serv.mib**.

***Table 3. MIB, MIB Objects and OIDs for Option 82***

| MIB | MIB Object | OID |
|---|---|---|
| **cjnipv4serv.mib** | cjnDHCPOpt82Sub1Enabled | 1.3.6.1.4.1.1751.2.43.2.5.5.1 |
| | cjnDHCPOpt82Sub2Enabled | 1.3.6.1.4.1.1751.2.43.2.5.5.2 |

# MAC Address Lock and Traps for Unknown Source Addresses

## Overview

If a source MAC address is locked at a port (statically configured), the switch filters frames that have that source MAC if they are received on any port in the same VLAN. The switch can also generate traps to identify all unknown source addresses. Traps for unknown source addresses are generated every intrusion trap timer interval. The default value of the timer is 30 minutes.

The switch keeps a history of intruding source MAC addresses. A history of 64 such addresses is stored in a software buffer at a time. The switch stores the source MAC address and sends a trap for an unknown MAC address, every intrusion trap timer interval. Once the MAC address is stored and the trap is sent, the switch does not send a trap for this MAC address again, until that MAC address is flushed from the buffer.

*** Note:** You can set the trap timer within a range of 60 to 1800 seconds (default) in one second intervals.

To enable traps for unknown source addresses, you must first enable the MAC Address Lock feature. You can enable this feature and traps for unknown source addresses by using the Web Agent, CLI, or SNMP.

## Web Agent Procedure

To use the Web Agent to enable the MAC Address Lock feature and traps for unknown source addresses:

1. Manually add the "permitted" MAC addresses to the Address Forwarding Table (AFT).

   For information on how to manually add MAC address to the AFT, see "Adding Entries to the AFT Manually" on page 21.

2. Open the Switch Port Configuration Web page for the port.

   For information on how to open this Web page, see "Configuring Switch Port Parameters" on page 24.

3. Set the **Allow Learning** field to **Disable**.

4. Set the **Known Mode** field to **Enable**.

   *** Note:** To prevent the flooding of frames that have unknown destination addresses, set the **Known Mode** field to **Enable** for all ports on the same VLAN as the port for which you are enabling MAC address lock.

5. Set the **Intrusion Trap** field to **Enable**.

6. Adjust the trap timer, if desired.

   For information on how to adjust the trap timer, see "Configuring Switch Port Parameters" on page 24.

7. Click **Apply**.

## CLI Commands

To use the CLI to enable the MAC Address Lock feature and traps for unknown source addresses:

1. Enter Global Configuration mode.

   The CLI displays the `Avaya (configure)#` prompt.

2. Use the following command to manually add the "permitted" MAC addresses to the Address Forwarding Table (AFT):

   **set aft entry <*mac address*> VLAN <*VLAN-id*> port-binding forward <*mod-port-spec*>**

3. Use the following command to disable learning on a port or port range:

   **set port allow-learning <*mod-swport-range*> disable**

4. Use the following command to enable known mode on a port or port range:

   **set port known-mode <*mod-swport-range*> enable**

   *** Note:** To prevent the flooding of frames that have unknown destination addresses, enter all ports on the same VLAN as the port for which you are enabling MAC address lock.

5. Use the following command to enable intrusion traps on a port or port range:

   **set port intrusion-trap <*mod-swport-range*> enable**

6. Use the following command to set the intrusion trap timer to other than the default setting:

   **set port intrusion-trap-timer <*mod-swport-range*> <*intrusion-trap-timer-value*>**

## SNMP

The MIB objects that you use to perform this procedure are located in **ProminetMib.txt**, version 5.2.

To use SNMP to enable the MAC Address Lock feature and traps for unknown source addresses:

1. Use the MIB objects that are listed in Table 6-8 to manually add the "permitted" MAC addresses to the AFT.

*Table 6-8. MIB, MIB Objects, and OIDs for Adding AFT Entries*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.2 | promL2AddressControlIndex | 1.3.6.1.4.1.2167.5.1.4.3.1.1 |
| | promL2AddressControlMacAddress | 1.3.6.1.4.1.2167.5.1.4.3.1.2 |
| | promL2AddressControlPortBinding | 1.3.6.1.4.1.2167.5.1.4.3.1.3 |
| | promL2AddressControlVlanID | 1.3.6.1.4.1.2167.5.1.4.3.1.4 |
| | promL2AddressControlPriority | 1.3.6.1.4.1.2167.5.1.4.3.1.5 |
| | promL2AddressControlPersistence | 1.3.6.1.4.1.2167.5.1.4.3.1.6 |

2. Use the MIB object that is listed in Table 6-9 to disable learning on a port.

*Table 6-9. MIB, MIB Object, and OID for Disabling Learning*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.2 | promSwitchPortLearningMode | 1.3.6.1.4.1.2167.5.2.1.1.4 |

3. Use the MIB object that is listed in Table 6-10 to enable known mode on a port.

*Table 6-10. MIB, MIB Object, and OID for Enabling Known Mode*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.2 | promSwitchPortKnownMode | 1.3.6.1.4.1.2167.5.2.1.1.7 |

4. Use the MIB object that is listed in Table 6-11 to enable intrusion traps on a port

.

*Table 6-11. MIB, MIB Object, and OID for Enabling Intrusion Traps*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.2 | promSwitchPortIntrusionTrap | 1.3.6.1.4.1.2167.5.2.1.1.19 |

# 7 Configuring Redundancy Options

## Overview

The Avaya Multiservice Switch can be configured with redundancy to provide fault tolerance.

### Supervisor Functions

The Avaya Multiservice Switch supervisor module manages the resources of the switch, provides access to these resources and supports a number of network protocols. These resources include configuration information, spanning tree topology, address forwarding tables, routing tables, and network statistics. Access is provided to these resources via console CLI (command line interface), Web interface, SNMP, and telnet.

### Redundant Supervisors

The redundant supervisor module is an auxiliary “standby” supervisor module that acts as a fault-tolerant supervisor in the event that the “Active” supervisor fails. Once the redundant supervisor is installed, loaded with the same software version as the Active supervisor, and synchronized, it is ready to act as a redundant or “standby” supervisor. If the Active supervisor does fail, the redundant supervisor assumes control of network operation. No user intervention is required for the Supervisor module failover. The management view is accessible without changing IP or MAC addresses. The event is logged and indicated via an SNMP trap. Notification of this change is provided by a console message and an event log message.

### Multiple Software Versions

Up to two software versions can be saved on the Avaya Multiservice Switch supervisor module.

## Redundant Switch Controller and Element

The Avaya Multiservice Switch can be configured with a redundant switch element module and a redundant switch controller module, for backup of both switch fabric components. In the event of a failure in a switch element or controller module, the redundant module will take over the function of the failed component.

## Virtual Router Redundancy Protocol (VRRP)

The Avaya Multiservice Switch supports Virtual Router Redundancy Protocol (VRRP), an IETF protocol designed to support redundant LAN routers, as well as load balancing of traffic. VRRP is transparent to host end stations. All configurations are done at the Avaya Multiservice Switch, no additional end station configurations are required. See the “Virtual Router Redundancy Protocol (VRRP)” section in Chapter 9, “Configuring IP Routing”, for more details.

## Hunt Groups

Ports within a Hunt Group by default are redundant to one another since Hunt Groups perform load balancing among the ports. The Hunt Group load-shares the traffic between two switches allowing the bandwidth to be multiplied. The use of Hunt Groups also increases reliability since the links behave as hot standby links to one another. If the traffic is shared over multiple links, and one of the links is "lost", the traffic will be automatically redistributed over the other links and the communications will continue without interruption See the “Hunt Groups” section in Chapter 4, “Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping” for more details.

## Redundant Power Supplies

Only two power supplies are required to support a fully-loaded Avaya Multiservice Switch. A third power supply can be installed to provide backup should one of the other two fail. The power subsystem provides N+1 power supply redundancy.

## Supervisor Failover conditions

The Active supervisor module fails over to the standby supervisor if one of the following events occur:

- Active Supervisor module removal
- Active Supervisor Software reset
- Active Supervisor Module Reset Push button
- Active Supervisor loses power
- Active Supervisor system crash either hardware or software

## Chapter Contents

The following information and procedures are provided in this chapter:


- Configuring Redundant Hardware
- Installing and Enabling Redundant Hardware
- Replacing the Primary Controller
- Replacing an Element
- Configuring Supervisor Module Redundant Ethernet Console IP Addresses
- Synchronizing the Active and Standby CPUs


# Configuring Redundant Hardware

The Avaya Multiservice switches provide a redundant backplane to ensure that should a Supervisor module, Switch Controller, or fabric element fail, it will continue to forward data properly. The redundant components are available as separate options.

## Redundant Switch Controllers and Elements

Controllers and Elements are located at the rear of the switches. When the redundant controller and element are installed, the backplane consists of the following parts (Figure 6-17or Figure 6-18):

- One Primary Controller
- One Redundant Controller
- Six Active elements
- One Redundant element

***Figure 6-17. Layout of the Redundant Backplane for P550R/P580 Chassis***

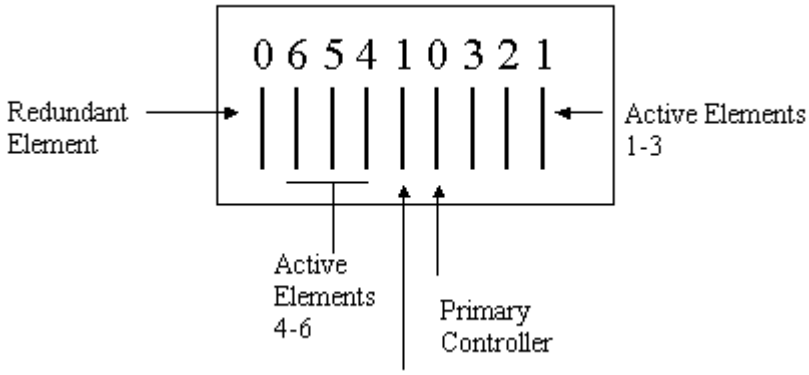
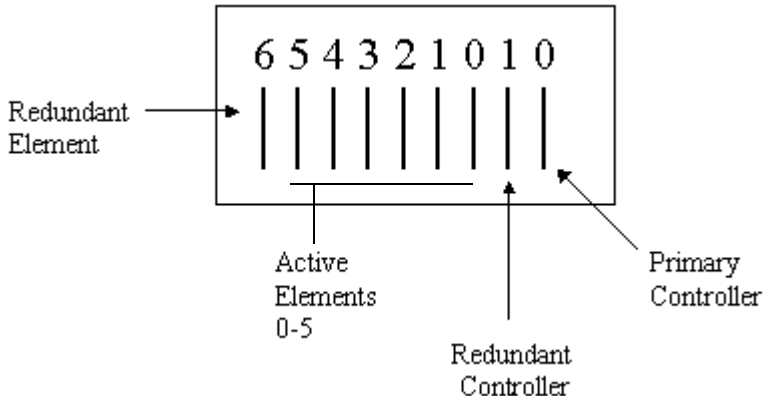



***Figure 6-18. Layout of the Redundant Backplane for P880/P882 Chassis***




The Avaya Multiservice switches are equipped with diagnostics to:

- Monitor the status of the Primary switch controller.
- Monitor the status of a Active element.
- Monitoring of Health Check status messages sent between the Active and Standby supervisors.

If the Active supervisor fails, the Standby supervisor assumes supervisor operation. Information about a failed Supervisor (CPU) displays in the CPU Redundancy Status Dialog Box window.

If the Primary controller fails, the redundant controller takes over switch controller operation. When an element fails, diagnostics run automatically to test the hardware. Information about a failed controller or element displays in the Switch Fabric Status window in the Web Agent. The redundant element takes over the function of the failed element until it is replaced.

*** Note:** In the event that the Primary switch controller fails, the switch will reset and record an entry of the event in the shutdown log.

If the Active element fails, the Active and Standby Supervisor modules can no longer communicate, or be synchronized. No health messages will be passed. However, the Standby Supervisor module will become Active if the current Active Supervisor module fails.

# Installing and Enabling Redundant Hardware

The standard switch configuration does not include a redundant controller or element. The correct process is to:

- Install the redundant hardware
- Enable the redundant hardware using either the Web Agent or the CLI.

After the redundant hardware is enabled, the applicable redundant component takes over if either a controller or any element fails.

# Installing Redundant Hardware

To install redundant hardware:

1. Turn off all of the switch power supplies.
2. Replace the Primary switch controller with the new switch controller. This ensures that the switch checks the status of the new switch controller.
3. Insert the previously Primary switch controller into the Redundant Controller Slot 1 (see Figure 6-17 for a P550/P580 or Figure 6-18 for a P880/P882).

   *** Note:** Controllers and elements are keyed to ensure that a controller is not inserted into an element slot.

4. Install the redundant element into the redundant element slot 0 for the P550R/P580, (see Figure 6-17), or slot 6 for the P880/P882, (see Figure 6-18).
5. Turn on the switch power supplies and log in.
6. Enable the Redundant Hardware as described in the next section.

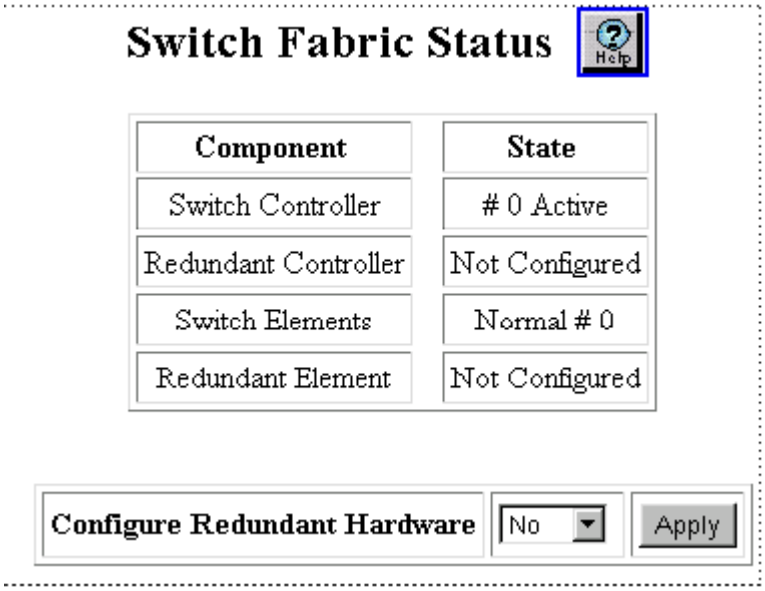
# Enabling Redundant Hardware

## Using the Web Agent

To enable redundant hardware using the Web Agent:

1. Select **Switch Fabric** from the **System > Configuration** group on the Web Agent window. The **Switch Fabric Status** dialog box opens. (Figure 6-19).

*Figure 6-19. Switch Fabric Status Dialog Box*



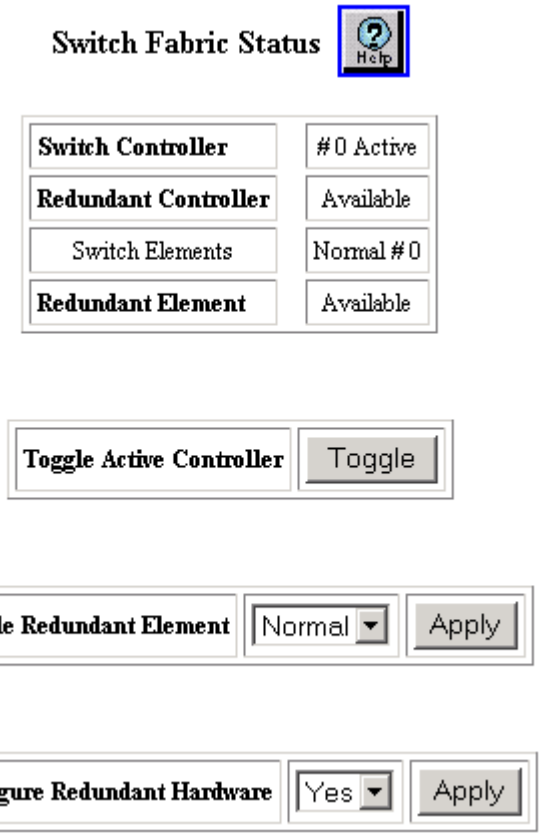

2. Select **Yes** from the **Configure redundant Hardware field** pull-down menu on the **Switch Fabric Status** dialog box (Figure 6-19).

3. Click **APPLY**. The Switch Fabric Status should now show the redundant controller and element **Available**. (Figure 7-4)

4. Save the configuration.

*** Note:** If you disable and then reenable redundant hardware after the Primary controller fails, the state of the failed controller changes from **Failed** to **Available**.

*Figure 6-20. Switch Fabric Status Dialog Box*




## Using the CLI

To enable the redundant hardware by using the CLI, enter the following command from **Enable/Configure** mode:

```
<configure># set fabric configure-redundant-
hardware enable
```

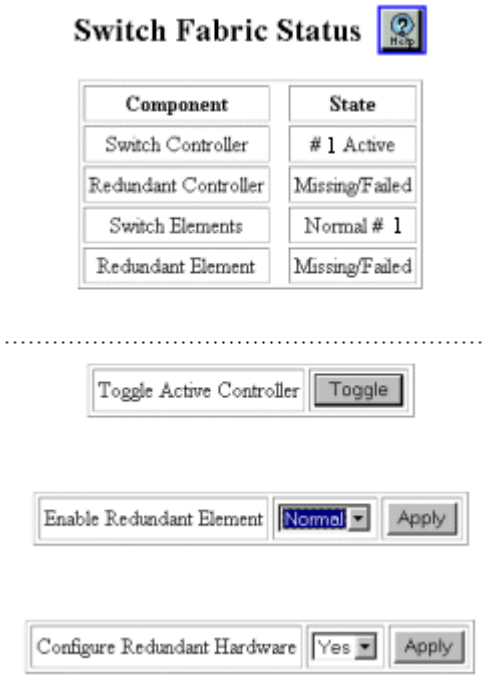
Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Replacing the Primary Controller

If a Primary controller fails, notification is provided by:

- An event log message
- An error message that displays in the **Switch controller** field.

***Figure 6-21. Switch Fabric Status Dialog Box***




If a redundant controller is installed in the switch and enabled, the switch resets and the redundant controller automatically takes over the operation of the failed Primary controller.

To replace the failed Primary controller:

1. Disable redundant hardware.
2. Copy the running config to the startup config.
3. Synchronize if you have redundant supervisor modules.
4. Power off the switch power supplies.

**WARNING**

To avoid bodily harm and equipment damage, you must power off the switch before you remove switch controllers or elements.

5. Replace the failed controller.
6. Power on the switch power supplies and login.
7. Enable the redundant hardware (see "Enabling Redundant Hardware" earlier in this chapter).
8. Re-select **Switch Fabric** from the **System > Configuration** group on the Web Agent window. The **Switch Fabric Status** dialog box re-displays with the Switch Controller field displaying:

   ```
   # 1 Active
   ```

# Replacing an Element

If an element fails, you are notified by:

- An event log message
- An error message that displays in the **Switch Elements** field

To replace a failed element:

1. Disable redundant hardware.
2. Copy the running config to the startup config.
3. Synchronize if you have redundant supervisor modules.
4. Power off the switch power supplies.

**WARNING**

To avoid bodily harm and equipment damage, you must power off the switch before you remove switch controllers or elements.

5. Power on the switch power supplies and login.
6. Enable the redundant hardware (see "Enabling Redundant Hardware" earlier in this chapter).
7. Replace the failed element.
8. Power on the switch's power supplies and login.

### Using the Web Agent

To enable the replacement element using the Web Agent:

1. Select **Switch Fabric** from the **System> Configuration** group on the Web Agent window. The **Switch Fabric Status** dialog box opens **(Figure 6-21).**
2. Select **Yes** from the **Configure Redundant Hardware** field pull-down menu.
3. Click **APPLY** to enable the redundant element.

   The Switch Elements field displays:

   ```
   Normal # 0
   ```

   This indicates that the redundant element is now enabled.
4. Save the configuration changes

### Using the CLI

To enable an element using the CLI, enter the following command from Configure mode:

```
> set fabric configure-redundant-hardware enable
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for more details about this command.

# Configuring Supervisor Module Redundant Ethernet Console IP Addresses

### Using the Web agent

If you need to communicate with both the Active and Standby Supervisors, configure an alternate Ethernet Console IP address for both. Configure an alternate IP address for both slot 1 and 2 CPU's, by using the Web Agent or the CLI.

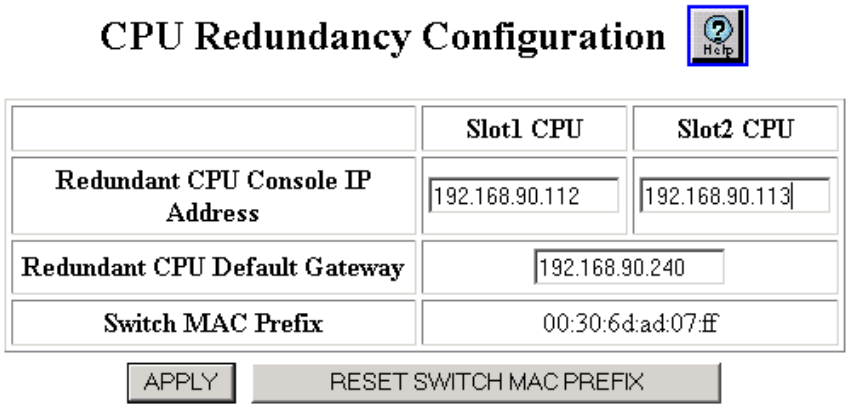
*** Note:** Do not Login to a Standby Supervisor module to manage the switch. The Standby Supervisor does not have accurate switch status information until it becomes the Active Supervisor.

Identifying the Active or Standby supervisor can be accomplished by looking at the LED display (marquee), or by opening the **System>Configuration>CPU Redundancy>Status/Statistics** group from the web agent, or by using the `show CPU status` CLI command.

To configure a redundant console IP address by using the Web Agent:

1. Select **Configuration** from the **System> Configuration > CPU Redundancy** group on the Web Agent window. The **CPU Redundancy Configuration** dialog box opens (Figure 6-22)

***Figure 6-22. CPU Redundancy Configuration Dialog Box***




2. Enter the internal IP addresses of the **slot 1 and slot 2 CPUs** in the **Redundant CPU Console IP Address** field. The addresses cannot be the same as the console IP or each other. The Gateway must be on the same subnet as the IP addresses. This sets the IP addresses for the Ethernet Consoles in slot 1 and slot 2 CPU's. The default values are 0.0.0.0.

3. Enter the redundant CPU default gateway IP address in the **Redundant CPU Default Gateway** field. This is the default gateway that the standby Ethernet console IP interface uses. It does not have to match the Active CPU's default gateway. The default value is 0.0.0.0.

4. The Switch **MAC Prefix** field displays the configured MAC prefix used to build the local MAC address for each routing interface. The first 36 bits of the switch MAC prefix make up the first 36 bits of this local MAC address. If the startup.txt does not set the switch MAC address, the supervisor's MAC address is used. Resetting this will cause it to be restored to the supervisor's MAC address. Only the Active supervisor uses this value. The default value is the manufacturer's supervisor MAC address.

5. Click **APPLY** to save your changes,

6. **RESET SWITCH MAC PREFIX** to reset the MAC prefix on your switch.

## Using the CLI

To configure redundant CPU IP addresses using the CLI, enter the following commands from **Enable/Configure** mode:

<configure># cpu_redundancy console {slot1/slot2} <ip address>

<configure># cpu_redundancy default-gateway <ip address>

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for more details about this command.

*** Note:** When the redundant CPU console IP address and default gateway are assigned and addresses are removed via the commands:

```
> no cpu_redundancy slot1
> no cpu_redundancy slot2
> no cpu_redundancy gateway
```

The router is no longer reachable and cannot be pinged or used by the Web Agent from redundant addresses. The initial console IP address is still usable.

# Synchronizing the Active and Standby CPUs

After installing the Active and Standby CPUs, synchronize them. Synchronization can be done by using either the Web Agent or the CLI.

*** Note:** If the Active Supervisor module and the Standby (redundant) Supervisor module are synchronized while the Active Supervisor module is being heavily used, TFTP transfers from the Active Supervisor module to the Standby Supervisor module may time out or fail.

Both Supervisor modules must be running the same software code and be in the same fabric mode. If you synchronize a Standby Supervisor module and the APP code, you must reset the switch before the Standby Supervisor module can load the new APP code. Otherwise, failover will result in the new Active Supervisor module running the old APP code or startup, configuration files.

After you synchronize Supervisor modules, the standby supervisor can only be accessed with the default passwords. The synchronization does not synchronize passwords.

*** Note:** P580 and P882 Supervisor modules must be in the same Fabric mode (1 or 2) to communicate and to synchronize.

## Synchronizing Process

The Active supervisor performs TFTP “puts” to the Standby supervisor to synchronize the Active and standby images and configurations. This process takes place over an internal subnet and VLAN. From the Active supervisor’s perspective this operation is the same as a TFTP configuration file upload.

During synchronization of the Active and standby, the boot code, app1 and app2 images will be synchronized. The following general rule is used when synchronizing images:

- If the standby's image version is lower than the Active's image version, the Active will overwrite the app code of the standby.

- If the standby's image version is the same as the Active's image and the sizes and checksums match, the Active will not attempt to synchronize the images.
- If the standby's image version is higher than the Active's image, the Active will not attempt to synchronize the images since the Active's image is lower than the standby's.

Once the standby and Active's images and Boot code have been synchronized, the Active supervisor will then do a TFTP put of the startup.txt and the.int files (critical files for a fast failover, e.g., spanning tree map of all blocked ports).

Once this step is done, and the standby supervisor is reset, the synchronization is complete.

## Supervisor Module Redundancy Status

The Active supervisor sends a health report message periodically to the standby (redundant) supervisor. If the standby supervisor is enabled, it responds with a health report reply.

- **Health Reports Sent** - Displays the number of health reports sent.
- **Health Reports Received** - Displays the number of health reports received.
- **Health Reports Timeouts** - Displays the number of health reports timeouts.
- **Health Reports Missed** - Displays the number of health reports missed.

Click REFRESH to reset all CPU redundancy statistics.

## Active and Standby Supervisor Mastership

**One Supervisor in Slot 1 -** The slot 1 supervisor module is Active. If a supervisor module is inserted into slot 2, module 1 remains active, and initiates Health Reports to the standby supervisor in slot 2.

**One Supervisor module in slot 2** - If a supervisor module is inserted into slot 1, the supervisor module in slot 2 remains the Active and initiates Health reports to the standby supervisor in slot 1. If the supervisor in slot 2 is removed/reset/failed or the switch is reset the supervisor in slot 1 becomes the Active and the supervisor in slot 2 becomes the standby. The supervisor in slot 1 then sends Health Reports to the supervisor in slot 2.

**Supervisor modules in slot 1 and slot 2** - Supervisor in slot 1 is the Active supervisor and initiates Health reports to the standby supervisor in slot 2. If the supervisor module in slot 1 is removed/ reset/failed the supervisor in slot 2 becomes the Active supervisor. If the supervisor in slot 1 is replaced, it remains as the standby supervisor and receives Health Reports from the Active supervisor in slot 2. If the supervisor in slot 2 is removed/reset/failed, the supervisor in slot 1 becomes the Active supervisor, and sends Health Reports to the supervisor in slot 2.(If the switch is power cycled, slot 1 supervisor is the Active supervisor, unless it has failed).

*** Note:** The TCP/IP interfaces have MAC and IP addresses. The standby supervisor becoming Active would assume the IP and MAC addresses that are used by the Active supervisor.

*** Note:** When a standby supervisor is installed in the switch there is a 45 second wait period before the standby supervisor is fully initialized.

**Do not remove the standby supervisor module at this time.**

**CAUTION**

## Using the Web Agent

To synchronize the Active and Standby Supervisor Modules by using the Web agent:

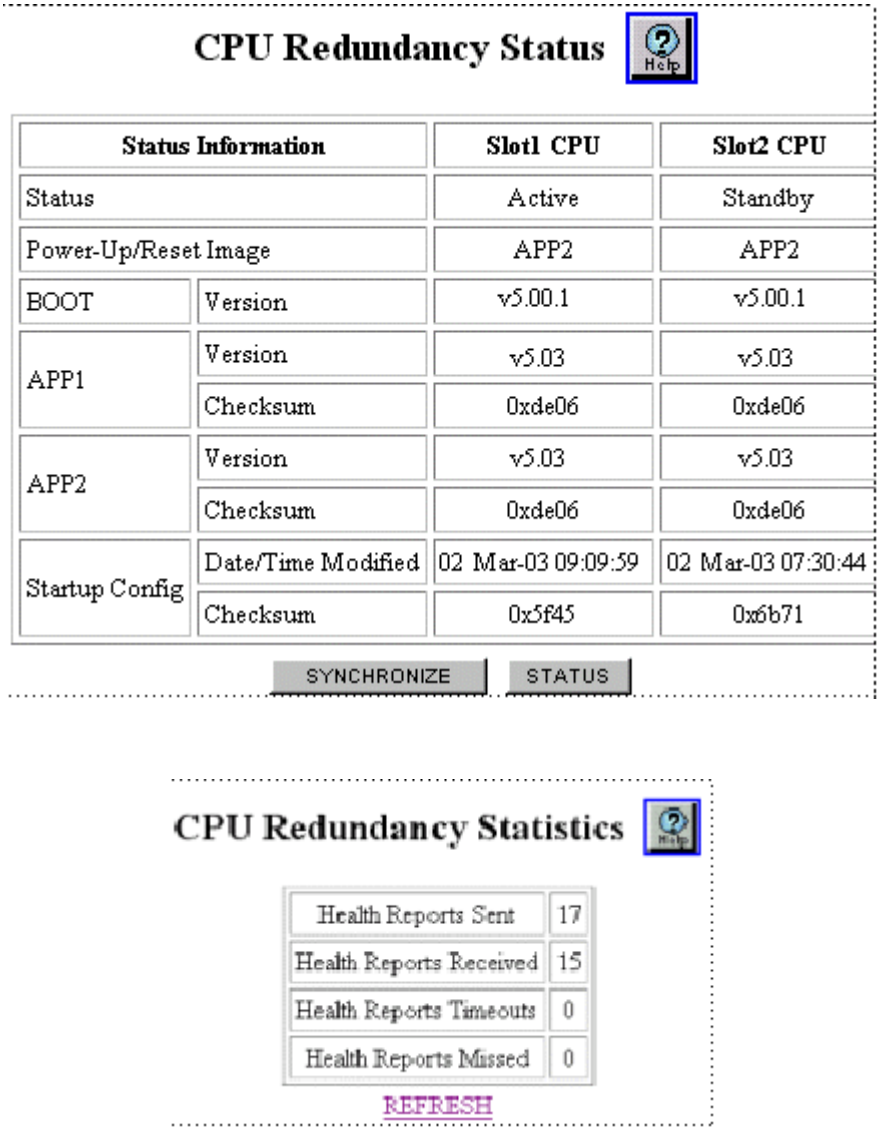
*** Note:** You must synchronize the Active and Standby Supervisor modules in order for the standby (redundant) supervisor to use the same configuration as the Active supervisor. Save your running configuration to startup configuration so if the Active supervisor fails, the current configuration information will not be lost. By synchronizing the two supervisors, it copies the startup configuration file to the standby supervisor. The standby supervisor module must be reset to run the new configuration.

The P580 and P882 Supervisor modules must be in the same Fabric mode to synchronize.

1. Copy the running configuration to the startup configuration from the Web agent System> System reset>Save button or the CLI command *config> copy run start*.

2. Select **Status/Statistics** from the **System> Configuration> CPU Redundancy** group on the Web Agent window. The **CPU Redundancy Status/Statistics** dialog box opens (Figure 6-23).

***Figure 6-23. CPU Redundancy Status/Statistics Dialog Box***




3. Ensure that the health messages between the supervisor modules are being sent and received by monitoring the CPU Redundancy Statistics window. Select the Refresh button to ensure the counters increment.

4. Synchronize the Active and Standby supervisors (CPUs). (Refer to Table 6-12 for more information on the **CPU Redundancy Configuration** dialog box parameters).

***Table 6-12. CPU Redundancy Status Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Status** | Displays the functional status of the CPU modules. |
| **Power-Up/ Reset Image** | Displays the image the CPU will use upon reset. |
| **APP1** | • **Version** - Displays the version of the image in application 1 (APP1) for each supervisor module. **Checksum** - Displays the checksum for the image running in APP1. |
| **APP2** | • **Version** - Displays the version of the image in application 2 (APP2) for each supervisor module. **Checksum** - Displays the checksum for the image in APP2. |
| **Startup Config** | • **Date/Time Modified** - Displays the date and time that the configuration (startup.txt) was modified.<br>• **Checksum** - Displays the checksum for the image in the Startup Config. |

5. Click **SYNCHRONIZE** to start the synchronization process.

6. Reset the standby supervisor from the CLI to initialize the changes.

*** Note:** If the 48-port mode is different on the Active and Standby Supervisor modules, the standby Supervisor module will automatically reset.

## Using the CLI

To synchronize the Active and redundant CPU's using the CLI. enter the following command in **Enable** mode:

```
># cpu_redundancy sychronize
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for more details about this command.

# 8 Configuring DNS Client

## Overview

This chapter provides an overview of the Domain Naming System (DNS) Client support and procedures for configuring DNS client support on the Avaya Multiservice switch.

## DNS Client Support

### Overview

DNS is a distributed database of name servers which supply name-to-address translations for DNS clients. The DNS servers collectively direct DNS Clients to the DNS Server responsible for a Name to Address mapping; and that Server provides the specific mapping being requested.

There are three types of DNS servers:

- The root name server — Located at the top of the DNS database tree. It contains pointers to the master name servers for each of the top-level domains. The root name servers handle the domains such as .COM, .EDU, .GOV, etc.
- The master name server — Located in the middle of the DNS database tree. It contains pointers to the individual name servers for each of the subdomains within its top-level domain.
- The individual name server — Located at the bottom of the DNS database tree. It contains detailed address information for the local hosts in the subdomain.

### Recursive vs. Iterative

The goal of DNS is to resolve a fully qualified domain name (FQDN) to an IP address. This work can either be done by the DNS server or the DNS client. These approaches are referred to as Recursive or Iterative, respectively.

In the Recursive approach, a client sends a query to the server. Assuming recursion is enabled, the server then looks for resolution first locally in its own database, then in its local cache, finally by going through the DNS tree until it finds a server that can give an authoritative answer to the query. In this model, the client is referred to as a Stub Resolver. Typically, Stub Resolvers are implemented on devices with limited resources such as embedded systems or Personal Computers.

The Avaya Multiservice switch is a Stub Resolver, i.e. it only supports a Recursive lookup not Iterative.

There are four most common answers a DNS server can provide are:

- **Authoritative** - a positive answer returned to the client with the Authoritative Answer (AA) bit set in the response.
- **Positive** - an answer that contains the resource record (RR) or list of RRs that match the query.
- **Referral** - an answer that contains a list of alternate servers the client can use to resolve the name. This type of answer is given if Recursion is not supported.
- **Negative** - this answer indicates that an Authoritative server reported that the name (or record type) does not exist in the DNS name space. The server can be the preferred server or, if recursion is enabled, that another server responded back to the preferred server with the authority bit set.

In the Iterative approach, the client sends a query to the server. If recursion is disabled, and the server cannot answer the query, the server will responds with a Referral answer. The client will then use that information to query another DNS server. This process will continue until a server responds with an Authoritative response.

## Sample walkthrough of a Recursive DNS query

Typically, a network will have a local DNS server which provides translations for devices in the local network. That server will also "know" the IP address of the Root servers. When a client attempts to communicate with a device by its name, the IP portion of the protocol stack will recognize that a name (not an address) has been specified. It will then contact the local DNS server and request the name be translated into an IP address. For example: if a user types **`ping www.avaya.com`**, that name will be sent to the local DNS server. If the DNS server has that information, it will respond with the appropriate IP address.

If the DNS server does not have that address translation, it will contact the root server using the IP address for that root server. In this example, it would use the IP address for the **.COM** root server.

Root servers do not have specific translations for names, but they do have the database of master name servers. The root server would the avaya.com master name server using the avaya.com IP address.

The root server would then send a request to the master name server requesting the translation. In small subdomains, a single DNS server may be adequate for servicing the subdomain and be able to translate all DNS requests. So the master name server may act as the individual name server by providing the translations.

In large subdomains, a single DNS server may be inadequate to handle all of the address translations. In these cases, the master name server may point to other individual name servers. In this case, we are pinging the web server **www.avaya.com**. Assume for this example that Avaya has a single DNS server for the entire subdomain of avaya.com. The avaya.com DNS server would use the IP address of the Avaya web server.

The client would then insert the IP address into the IP packets going to the destination. In this example, it would put the IP address in the HTTP packet going to the Avaya web site.

The benefit of using DNS is that you need only know the name of the server instead of the IP address for which you are trying to communicate. Also, if the IP address of the server changes, you need only update the DNS database.

Many vendors provide DNS servers. Consult the DNS Server vendor's documentation for information on configuring the DNS server. Virtually every IP protocol stack includes DNS client capabilities. The Avaya multiservice switch is a DNS client only.

## DNS Client on the Avaya Multiservice Switch

The Avaya Multiservice switch has DNS client capabilities that work in conjunction with the Command Line Interface (CLI). This feature is useful for testing connectivity (ping and traceroute) as well as copying files from TFTP servers.

It is not meant for use with the normal operation of the Avaya switch. Therefore, you should not use a DNS name to specify the location of the Avaya Multiservice switch's RADIUS server, SNTP Time server, etc. These parameters must be specified as IP addresses.

However, DNS does work for the Avaya Multiservice Switch's Help File HTTP server.

In order for the DNS client functionality to work, it must be enabled on the switch and at least one name server IP address must be specified.

The following DNS Client features are supported:

- The DNS Client on the Avaya Multiservice switch is Stub Resolver (i.e. it does not support Iteration). This means that referral answers will be discarded. A Recursive DNS server must be used if you intend on using FQDN for which the configured DNS servers do not have resource records.
- Up to six DNS name servers can be configured.
- Up to six default DNS Domain Suffixes can be configured.
- When DNS is enabled, DNS names can be used in place of IP addresses for `ping`, `telnet`, `connect, traceroute and copy tftp` CLI commands.
- The DNS client name can consist of up to 255 characters.
- A single label within a DNS client name can consist of 63 characters.

Once enabled, you have the option of specifying a DNS suffix to add to unqualified host names. If so, you need only type the host name, in place of the IP address, without the suffix when entering commands. The suffix will be appended to host names that have no suffix.

For example: You can specify the avaya.com suffix. So when you want to ping **hostA** in the avaya.com domain, you need only type the host name without the suffix.

Avaya(Configure)# **ping hostA**

instead of:

Avaya(Configure)# **ping hostA.avaya.com**

## Order of Operations for DNS on the Avaya Multiservice Switch

You can configure up to six DNS servers and up to six DNS suffixes. When you use a name instead of an IP address in a command, the Avaya Multiservice switch will first check to see if the name is a fully qualified domain name (ex: hostA.avaya.com). If it is, this will be sent to the first DNS server in the list of servers.

If it is not a fully qualified domain name (ex: just hostA) and a suffix(es) has been specified, the first suffix will be appended to the name; and then sent to the DNS server. If no suffix(es) is configured, it will be sent as is for resolution.

If the server cannot resolve the name, the Avaya Multiservice switch will use the same method with the second configured suffix. Once it has exhausted the configured DNS suffixes, it will attempt the query with the second DNS server.

This process will continue until the name is either resolved, there are no more DNS servers in the list, or the DNS server returns an error. Table  lists the error messages and their meanings that you may encounter when using the DNS client.

*Table 6-13. DNS Error Codes*

| Error Message | Explanation |
|---|---|
| **Bad ARGS** | indicates that DNS is Disabled but the user entered a host name. |
| **Name Too Long** | the name sent is too long. RFC 1034 limits DNS names to 255 characters. |
| **Bad Name** | indicates that the name was in some way invalid |
| **Label Too Long** | indicates that the label of a DNS name was too long. RFC 1034 limits labels to 63 octets. |
| **Time-out** | indicates that the DNS query has expired. This implies that the query could not be answered at the present time. |

| *Table 6-13. DNS Error Codes continued* | |
|---|---|
| **Error Message** | **Explanation** |
| **Server Failure** | indicates that the DNS server is unable to answer due to a failure on the DNS server itself. |
| **Non-Existent Name** | indicates that the DNS server authoritatively claims that the DNS name does not exist. |
| **NIY** | Indicates the DNS server does not support the requested service. You may have specified the correct DNS server but the server has not yet been configured to respond to DNS queries. |
| **Refused** | indicates that the DNS server refuses to answer the query for administrative reasons. Possibly due to security implementations on the DNS server. |
| **No RRs** | indicates that the DNS server authoritatively claims that there are no RRs that match the specified name, type and/or class. |
| **No Recursion** | indicates that one of the configured DNS servers does not support Recursion. |
| **Irrelevant** | indicates that a response message was received that does not match the query sent. |

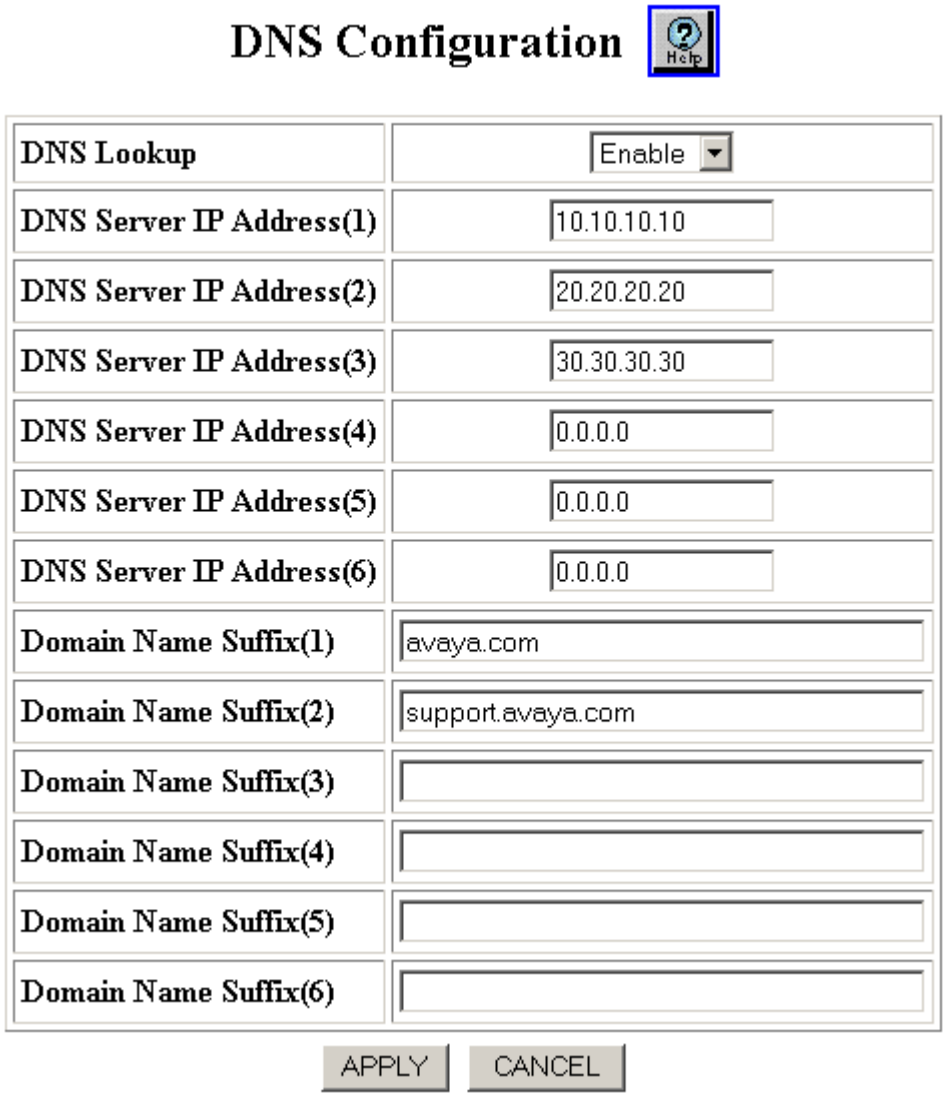
You can configure DNS client from the Web Agent or the CLI.

## Using the Web Agent

To configure a DNS client by using the Web Agent:

1. Select **DNS** from **System> Administration** group on the Web Agent window. The **DNS Configuration** dialog box opens (Figure 6-24).

*Figure 6-24. DNS Configuration Dialog Box*




2. Select **Enable** from the **DNS Lookup** field pull-down menu to enable DNS on the switch.

   *** Note:** When DNS is enabled and configured, you can enter DNS names in place of IP addresses for the following CLI commands. Again, DNS is for use with the CLI only for testing connectivity and

copying files from TFTP servers, not the normal operation of the Avaya Multiservice switch.

- ping
- telnet
- connect
- trace (traceroute)
- copy tftp

3. Enter the DNS server IP address for each DNS server in the **DNS Server IP Address** fields (fields 1-6).
4. Enter the domain name suffix for each DNS server in the **Domain Name Suffix** fields (fields 1-6).
5. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Using the CLI

The following commands configure DNS client using the CLI. (You must be in **Global Configuration** mode):

**Enabling & Configuring DNS parameters:**

```
ip domain-lookup (to enable DNS Client)
ip name-server <a.b.c.d> (to add a DNS server address)
ip domain-list <name> and ip domain-name <name> (to add a DNS suffix)
```

**Disabling & Clearing DNS parameters:**

```
no ip domain-lookup (to disable DNS Client)
no ip name-server <a.b.c.d> (to remove a DNS server address)
no ip domain-list <name> (to remove a DNS suffix)
no ip domain-name <name> (same as no ip domain-list)
```

**Display DNS configuration:**

```
show hosts (display the DNS Client configuration)
```

## CLI Example

The following CLI example enables DNS, configures three DNS servers, two suffixes, and then displays the DNS configuration:

```
Avaya(configure)# ip domain-lookup
DNS domain name lookup is ENABLED.
```

```
Avaya(configure)# ip name-server 10.10.10.10
Added name server '10.10.10.10' to the name server
list.
Avaya(configure)# ip name-server 20.20.20.20
Added name server '20.20.20.20' to the name server
list.
Avaya(configure)# ip name-server 30.30.30.30
Added name server '30.30.30.30' to the name server
list.
Avaya(configure)# ip domain-list avaya.com
Added domain name 'avaya.com' to the domain name
list.
Avaya(configure)# ip domain-list support.com
Added domain name 'support.avaya.com' to the domain
name list.
Avaya(configure)# show hosts

DNS domain name lookup is ENABLED.

Configured DNS name servers:
        10.10.10.10
        20.20.20.20
        30.30.30.30

Configured DNS default domain names:
        avaya.com
       support.avaya.com
```

# 9 Configuring IP Routing

## Overview

The Avaya Multiservice Switch supports the full suite of IP protocols for unicast and multicast packet routing and control. It is compatible with the installed base of IP routers and does not require changes to software in hosts or other routers. For Unicast, the Switch supports OSPF, RIP, and RIP2 interior gateway protocols. For Multicast, it implements IGMP, and DVMRP

The following information and procedures provided in this chapter pertain to Licensed layer 3 module configurations only:

- Routing Function
- Hardware Requirements for IP Routing
- Software Requirements for IP routing
- Minimum IP Routing Configuration Requirements
- Routing Configuration Quickstart
- Displaying Existing IP Interfaces
- Creating and Assigning IP Interfaces to the VLAN
- Enabling IP Forwarding (Routing) Global Parameters
- Access Lists (also called Access Control Lists or ACLs)

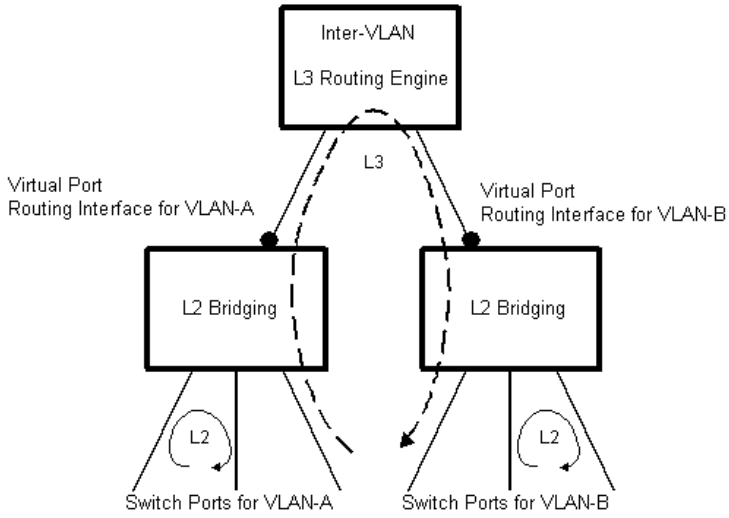
## Routing Function

The Routing function is logically independent from and sits “on top” of the Layer 2 VLANs. The function of the Inter-VLAN router is to route traffic between VLANs (subnets). The router has an “interface”, or “virtual port”, for each VLAN that it is routing traffic.

This interface is configured similarly to a physical interface, but is not associated with any particular physical interface.(Figure 9-1)

For more detailed information on the switch routing operations, see "Routing with Layer 2 and Layer 3 Modules", in Chapter 1, "*Introduction*".

***Figure 6-25. Intra and Inter VLAN Bridging and Routing***




## Hardware Requirements for IP Routing

To configure your switch as an IP router, you must configure your switch with the following hardware:

- Layer 3 supervisor module

*** Note:** Licensed layer 3 80-series media modules are recommended for best routing performance.

## Software Requirements for IP routing

To configure your switch as an IP router, with 80 series modules (Supervisor and Media modules) you must configure your switch with a minimum of version 5.0 and above.

## Minimum IP Routing Configuration Requirements

Your switch must be configured as follows to successfully create IP routing:

- VLANs (subnets) have been created to address current or future network configurations, or if you plan to expand your current network.
- Assign an IP address, and subnet mask to each configured IP interface.
- IP unicast forwarding must be globally enabled.
- At least one routing protocol (RIPv1,RIP v2, OSPFv2) must be enabled, if communication between routers is necessary.

## Routing Configuration Quickstart

This section provides an overview of the how to configure the Avaya Multiservice switch as a IP router.

To configure the switch as a IP router:

1. Ensure that Physical port parameters and cabling are correctly configured before creating VLANs, Chapter 5, "*Configuring Port Parameters*".
2. Create a VLAN (each VLAN is an IP subnet)"*Creating and Implementing VLANs*," in Chapter 4, "*Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping Overview*"
3. Assign switch ports to the VLAN."Configuring Switch port Parameters", in Chapter 5, "*Configuring Port Parameters*".
4. Configure an IP interface, IP address and subnet mask, for each VLAN and associated subnet.
5. Globally enable IP Forwarding (Routing)
6. Enable the routing protocol on an interface
7. Specify how the router will communicate with other routers, by configuring RIPv1, RIPv2 or OSPF v2 parameters.

*** Note:** the IP interfaces should be set to the ADMIN state "Down"

8. Set the IP interface Admin State to "Up"

# Displaying Existing IP Interfaces

When you create an IP interface, you activate a location in the switch that communicates between IP and the embedded software of the switch. You can create an IP interface using either the Web Agent or the CLI.

## Display Existing IP interfaces Using the Web Agent

To display, modify, delete a previously created IP interfaces or to create a new IP interface using the Web Agent:

1. Select **Interfaces** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Interfaces** dialog box opens (Figure 6-26- split in three due to size).

***Figure 6-26. IP Interfaces Dialog Box***

IP Interfaces

| Select | State | Name | Interface Type | Admin. State | VLAN | Network Address | Mask |
|---|---|---|---|---|---|---|---|
| ☐ | UP | Console | Ethernet LAN | UP | Ethernet-Console | 10.0.8.203 | 255.255.255.0 |
| ☐ | UP | vlan34int | Ethernet LAN | UP | vlan34 | 192.3.24.10 | 255.255.255.0 |
| ☐ | UP | vlan33int | Ethernet LAN | UP | vlan33 | 192.3.23.10 | 255.255.255.0 |
| ☐ | UP | vlan32int | Ethernet LAN | UP | vlan32 | 192.3.2.10 | 255.255.255.0 |
| ☐ | UP | vlan31int | Ethernet LAN | UP | vlan31 | 192.3.1.10 | 255.255.255.0 |
| ☐ | INACTIVE | dave | Ethernet LAN | UP | Default | 0.0.0.0 | 0.0.0.0 |
| ☐ | UP | Internal-Network | N/A | UP | Internal-Network | 10.2.2.1 | 255.255.255.224 |

APPLY | CREATE | DELETE | CANCEL

| MAC Format | ARP Timeout | Directed Broadcast | IP Routing | RIP | OSPF | Multicast Protocol |
|---|---|---|---|---|---|---|
| Ethernet V2 | 14400 | Enable | Mgmt Only | Disable | Disable | N/A |
| Ethernet V2 | 14400 | Enable | Routing/Mgmt | Disable | Disable | None |
| Ethernet V2 | 14400 | Enable | Routing/Mgmt | Disable | Disable | None |
| Ethernet V2 | 14400 | Enable | Routing/Mgmt | Disable | Disable | None |

| Proxy ARP | ICMP Redirect | NetBIOS UDP Rebroadcast | VRRP | BOOTP/DHCP Relay Gateway |
|---|---|---|---|---|
| Disable | Disable | Disable | Disable | Enable |
| Disable | Enable | Disable | Disable | Enable |
| Disable | Enable | Disable | Disable | Enable |
| Disable | Enable | Disable | Disable | Enable |

2. To modify an IP interface first click on **Select**, to select the specific interface, modify the parameter(s), and then click on **APPLY** or **CANCEL** to restore previous settings.

*** Note:** If you modify the ARP Timeout value, the new value **does not** take affect when you click on **APPLY**.You must, in addition to changing the ARP Timeout value, change the Admin State to **Down,** then change the ARP Timeout value, and then change the Admin state back to **Up** for that Interface.

This procedure can be done when you change the ARP Timeout value. If not already selected, select **Interfaces** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Interfaces** dialog box opens (Figure 6-26-).

Click on the **Select** checkbox for the Interface, change the **Admin State** to **Down**, then click on **APPLY**. Again select the interface, enter the new value of the **ARP Timeout** period, and change the Admin State parameter to **UP**, then click on **APPLY**.

3. To delete an IP interface first click on **Select,** to select the specific interface then click on **DELETE**.

4. Refer to Table 6-14 for an explanation of the **IP Interfaces** dialog box parameters.

# Creating and Assigning IP Interfaces to the VLAN

## Web Agent Procedure

After you have set up a VLAN, you must create the IP interface that your VLAN and your subnet uses to communicate with each other. While creating the IP interface, you must assign it to the VLAN. The last step is to enable IP forwarding (Routing) global parameters.

1. Select **Interfaces** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Interfaces** dialog box opens (Figure 6-26).

2. Click **CREATE**. The **Add IP Interface** dialog box opens (Figure ).To create a new IP interface and assign it to a VLAN.

***Figure 6-27. Add IP Interface Web Screen***

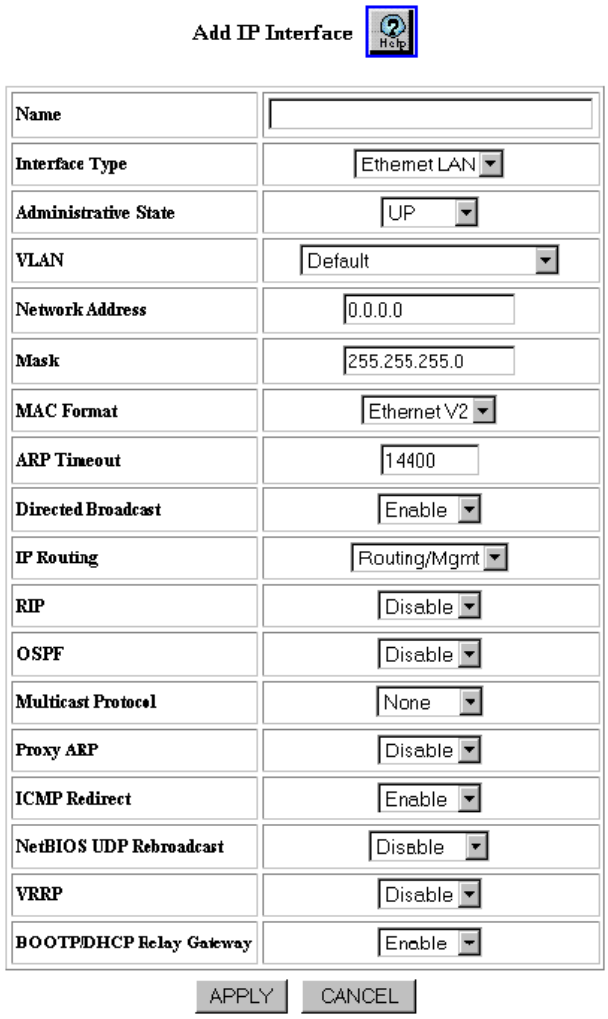


*Table 6-14. Add IP Interface Web Page Fields*

| Parameter | Allows you to... |
|---|---|
| **Name** | Enter a unique, alphanumeric name for the interface (maximum 28 characters) |
| **VLAN** | A pull down menu that associates a VLAN with this IP Interface.<br>**Note:** The way that you configure a port(s) to a VLAN determines the IP Routing option that you select for the interface. Use the following options to configure the appropriate interface:<br>• **Default** - Selects the default VLAN.(VLAN ID=1)<br>• **Discard** - Selects the VLAN to be discarded.(VLAN ID= 4097)<br>• **VLANs-** A list of all VLANs created on the switch.<br>*** Note:** The following two parameters, **Ethernet-Console** and **Serial-Console** are special IP interface settings, and are not part of the normal routed data path. Do not configure routing only or routing and management for the serial interface or the Ethernet Console, configure both for management only.<br>• **Ethernet-Console** - Creates an IP interface and assigns the IP address to the Supervisor's Ethernet port.<br>• **Serial Console** - Creates an IP interface and assigns the IP address to the Supervisor's serial port (RS232). This is necessary if you are using PPP to connect to the supervisor's serial port. |
| **Interface Type** | Ethernet LAN or NBMA.<br>*Non-Broadcast Multi-Access* (NBMA) IP Interfaces. Makes it possible for the switch to exchange routing information over nonbridged connections (routed virtual switch ports (VSPs))<br>NBMA functionality was added to RIP and OSPF routing protocols on the Avaya Multiservice switch software. |

*Table 6-14. Add IP Interface Web Page Fields continued*

| Parameter | Allows you to... |
|---|---|
| **Administrative State** | Specify the administrative state of the interface. Options include:<br>• **UP** - The interface is active.<br>• **DOWN** - The interface is inactive. |
| **Network Address** | Enter the network IP address for the selected interface. |
| **Mask** | Enter the subnet mask for the interface. |
| **MAC Format** | Select the MAC address format for the interface.<br>Options include:<br>• Ethernet V2<br>• Simple Network Access Protocol (SNAP) |
| **ARP Timeout** | Enter the timeout period for Address Resolution Protocol (ARP) in seconds.The ARP Timeout value is the period of time the switch will wait for data from a station, if no data is received, the station is deleted from the ARP Table.<br>The default is **14,400** seconds (4 hours). |
| **Directed Broadcast** | When the IP Directed Broadcast feature is Enabled, it allows a Network Directed Broadcast (unicast IP address with the Host ID set to all One's) to be forwarded by the router on the selected interface. The default is **Enable.** |
| **IP Routing** | Select enable or disable IP routing on the interface. Options include:<br>• **Routing/Mgmt** (Default) - Enables you to manage the switch, from the Command Line Interface (CLI) or the Web Agent, and configure IP routing for the switch.<br>• **Mgmt Only** - Enables you to manage the switch, however, IP routing is disabled for this interface.<br>**Note:** Do not enable routing protocols on an interface configured for Mgmt Only since the interface will act as an end point and will not pass traffic.<br>• **Routing Only** - IP routing is enabled on the interface, but you cannot manage the switch through the interface. Routing Only interfaces do not permit management traffic destined for local interfaces but do allow all other traffic including management traffic destined for interfaces on other switches. |

*Table 6-14. Add IP Interface Web Page Fields continued*

| Parameter | Allows you to... |
|---|---|
| **RIP** | Enable or disable RIP. The default value is **Disable**. |
| **OSPF** | Enable or disable OSPF. The default value is **Disable.**<br>**Note:** To Enable OSPF, The Admin State of the IP interface must be set to down. Enable OSPF and then set the Admin State to up. |
| **Multicast Protocol** | Specify the multicast protocol for the interface. Options include:<br>• None (Default)<br>• DVMRP<br>• IGMP<br>*** Note:** By Default, multicast forwarding is disabled. To enable multicast forwarding go to the IP Global Configuration page. |
| **Proxy ARP** | Enable or disable Proxy ARP. The default value is **Disable**. |
| **ICMP Redirect** | Enable or disable ICMP Redirect (IDRP). The default value is **Enable**. |
| **NetBIOS UDP Rebroadcast** | Enable or disable NetBIOS UDP Rebroadcasts. The default value is **Disable.** |
| **VRRP** | Enable or disable Virtual Redundancy Router Protocol. The default value is **Disable**. |
| **BOOTP/DHCP Relay Gateway** | Enable or disable the BOOTP/DHCP Relay Agent. The default value is **Enable**. |

## Using the CLI

Using the CLI to create an IP interface requires two CLI commands.

1. Enter Configure mode.
2. Create an Interface Name first.

<configure># Interface <Interface_name> type <ethernet or nbma>

Example: Interface myif type ethernet

3. Assign an IP address to the interface.

<confg-if:myif># IP Address <ip-address> <network mask>

Example: (config-if:myif)# ip address 192.168.97.1 255.255.255.0

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Enabling IP Forwarding (Routing) Global Parameters

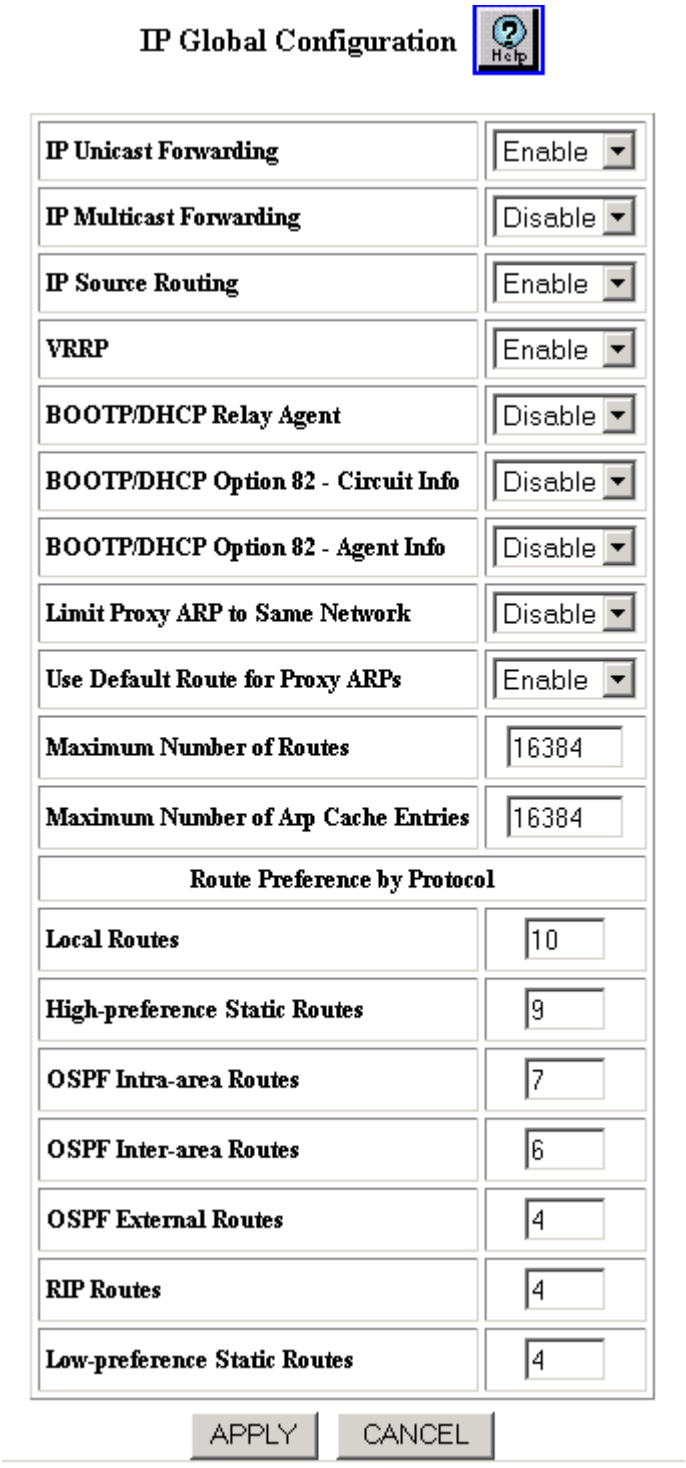
You can enable IP Unicast Forwarding (Routing) Globally using either the Web Agent or the CLI.

## Enabling IP Routing Using the Web Agent

To enable IP routing using the Web Agent:

1. Select **Global Configuration** from the **Routing > IP > Configuration** group on the Web Agent window. The I**P Global Configuration** dialog box opens (Figure 6-28).

*Figure 6-28. IP Global Configuration Dialog Box.*



Refer to Table 6-15 to configure the **IP Global Configuration** dialog box.

***Table 6-15. IP Global Configuration Parameters***

| Parameter | Allows you to... |
|---|---|
| **IP Unicast Forwarding** | **Disable** IP Unicast Forwarding. Must be enabled for Unicast Forwarding. The default setting is **Enable**. |
| **IP Multicast Forwarding** | **Enable** IP multicast forwarding on a global basis. Must be enabled for Multicast Routing or Forwarding. The default setting is **Disable**. |
| **IP Source Routing** | **Disable** IP source routing globally. The default setting is **Enable**. |
| **VRRP** | **Disable** VRRP globally. The default setting is **Enable**. |
| **BOOTP/DHCP Relay Agent** | **Enable** Client requests for an IP address and forwards their requests to a server. This agent also relays responses from the server to the client. The default setting is **Disable**. |
| **BOOTP/DHCP Option 82-Circuit Info** | **Enable** This sub-option 82 allows the sending of an agent-local identifier of the circuit (slot/physical port number) for a BootP/ DHCP client-to-server DHCP request. The default setting is **Disabled.** |
| **BOOTP/DHCP Option 82- Agent Info** | **Enable** This sub-option 82 allows the Avaya Multiservice switch to send its IP address and System name along with the BootP/ DHCP client-to-server request. The Default setting is **Disabled** |
| **Limit Proxy ARP to Same Network** | **Enable** Proxy ARP on the same network. When enabled, the router responds to ARP requests when the source and target IP address are in the same IP network and different IP subnets. When disabled, the router responds to ARP requests when the source and target IP address are in different networks. The default setting is **Disable**. |
| **Use Default Route for Proxy ARPs** | **Disable** the use of the default route on your switch as the route for Proxy ARPs. For example, if you have a default route configured to reach the 0.0.0.0 IP address, then any ARP request that does not match any of the other routes in your IP routing table will automatically go to this default route. The default setting is **Enable**. |
| **Maximum Number of Routes** | Enter the maximum number of routes that you want added to the routing table. The default number of routes is **16384**.<br>**Note:** These routes refer only to IP Unicast entries. |
| **Maximum Number of ARP Cache Entries** | Enter the maximum number of ARP cache entries. ARP entries refers to the space available for the IP address table. When you increase the number of entries, it may cause the table to be relearned more frequently. Consequently, it will make address space usage more efficient. The default maximum number of entries is **16384**. |

*Table 6-15. IP Global Configuration Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **Route Preference by Protocol** | This section describes the routing preferences set up according to the network administrator's preferences. These preferences are normally set up using the most to least trust. For example, local routes are normally considered to have *more trust* or a *higher preference*, while OSPF external routes are considered to have *less trust* or a *lower preference*. These preferences can be overridden, but careful consideration must be given when setting each.<br>**Note:** Local Routes must always have the higher preference.<br>**Note:** **Do not** change the Prerferences unless you are certain of the consequences. Incorrect Preference settings can cause the switch to stop all routing. |
| **Local Routes** | Enter a preference value for local routes.<br>**Note:** Local Routes must always have the higher preference. |
| **High-Preference Static Routes** | Enter a preference value for High preference static routes. |
| **OSPF Intra-area Routes** | Enter an OSPF intra-area route. A lower number indicates a lower preference for the path. |
| **OSPF Inter-area Routes** | Enter the inter-area paths to destinations in other OSPF areas. These are discovered through the examination of received summary Link State Advertisements (LSA). Enter a number to specify your path cost. A lower number indicates a lower preference for the path. |
| **OSPF External Routes** | Enter the number of external paths to destinations external to the Autonomous System (AS). These are detected through the examination of received AS external LSAs. Enter a number to specify your path cost (preference). A lower number indicates a lower preference for the path. |
| **RIP Routes** | Enter the number of RIP routes to use the hop count as a metric. Hence, to specify a preference for a RIP route, you need to enter a lower number (path cost). |
| **Low-Preference Static Routes** | Enter a preference value for Low preference static routes. |

2. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

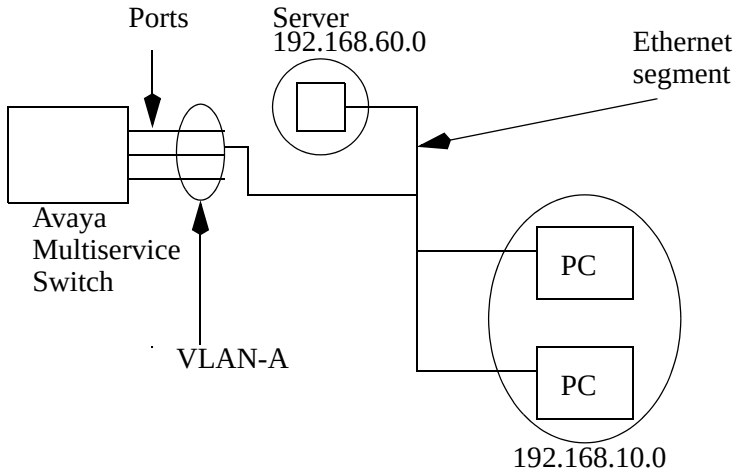
## IP Multinetting

You can set up a configuration of multiple subnets, and IP interfaces on a single VLAN. This is also referred to as **IP Multinetting**. A network is said to be multinetted when multiple logical groups of computers are brought together within a single broadcast domain. In the example (Figure 9-4), two separate networks are brought together in VLAN-A allowing computing resources on network

192.168.10.x to communicate with computing resources on network 192.168.60.x without having to go through a router. To create a multinetted network, you must assign multiple subnets to a VLAN.

*** Note:** Only one subnet can be BootP/DHCP Gateway. The second subnet must use Static IP addresses.

***Figure 6-29. Multinet Diagram***




## Creating a Multinet Interface

To create a multinet interface:

1. Select **Interfaces** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Interfaces** dialog box opens (Figure 6-26).
2. Select **CREATE**. The **Add IP Interface** dialog box opens (seeFigure ).
3. Enter a name for the interface in the **Interface** field.
4. Select a VLAN for this multinet interface from the **VLAN** field pull-down menu.
5. Enter the network address associated with this interface in the **Network Address** field.
6. Select **CREATE** from the bottom of the **Add IP Address** dialog box. The **IP Interfaces** dialog box re-opens with the new interface name listed in the Interface field.
7. Repeat steps 2 through 6 for any other interfaces that you want to associate with the same VLAN.

*** Note:** You must have a different network address for each new multinetting interface that you create for the same VLAN.

*** Note:** The first IP interface that has the BootP/DHCP Relay Gateway enabled will be the relay.

## Access Lists (also called Access Control Lists or ACLs)

The following information is provided in this section:


- Access Control List Overview
  - Standard vs. Extended ACLs
  - Naming Conventions for ACLs
  - How Packets are Processed
- Creating Access Lists
  - Creating Standard Access Rules
  - Creating Extended Access Rules
- Activating Access Lists
  - Activating Access Lists Using the Web Agent
  - Activating Access Lists Using the CLI
  - Example: Filtering Web Traffic Using an Access Rule
- Optimizing Performance when Using an Access Control List
  - How to Optimize Performance when using ACLs
  - Evaluate System Performance
  - Enable Routing at the Module
  - Design Safe, Efficient ACLs
  - Identify the Ports
  - Configuring Hash Mode
  - Managing F-chip Memory

# Access Control List Overview

An Access Control List (ACL) is a group of Access Control Rules. Access Control Rules are used to describe *how* to forward (route) packets, as opposed to where to forward them. The *how* can be to forward the packet with a specific priority(0-7), forward the traffic with an un-changed priority, or filter packets (drop).

ACLs provide the mechanism to prioritize traffic flows through the router and the network. This traffic flow management is commonly referred to as Quality of Service (QoS). Refer to Chapter 21 for more information on QoS.

## Standard vs. Extended ACLs

A “Standard” ACL allows you to prioritize traffic by the Source IP address.

An “Extended” ACL provides greater control over what traffic is prioritized. Extended ACLs can use any or all of the following parameters:

- Source IP address
- Destination IP address
- TCP/UDP Source port
- TCP/UDP Destination port.
- Protocol ID (RFC1700)

These five parameters are referred to as a “5 Tuple”. Source and/or Destination addresses allow you to prioritize traffic between any combination of host, subnet, and network addresses.

Further, if you specify source and/or destination TCP/UDP port, you can prioritize specific traffic between hosts on two different networks. For example, you could increase the priority of Voice Over IP (VoIP) traffic between two subnets in a call center by specifying the UDP port number used by the phone system.

*** Note:** If you specify TCP or UDP port numbers, you must specify Protocol ID 6 or 17 respectively. Failure to specify the Protocol ID number will result in an error message and the ACL will not be created.

Protocol ID allows you to prioritize traffic based on the Protocol ID number. RFC 1700 lists Protocol ID numbers. You could, for example, block all RSVP traffic (Protocol ID 46) through the router.

## Naming Conventions for ACLs

The Avaya Multiservice switch supports ACL names up to 32 characters (Alpha-Numeric). Spaces are allowed in the names but are not recommended. Instead of spaces, use the underscore "_" character.

ACL Names are entered when you create a rule. By using the same ACL Name for multiple rules, you are effectively creating a list of rules. The Access List Index determines the order of rules in the list. For that reason, when you create a rule, you give the rule the Access List Name and the Access List Index. No two rules in a list may have the same index.

If you create rules with ***different*** ACL Names, you have created different lists. This is useful when you need more than one ACL. For example, you may have one ACL for normal working hours, one ACL for nighttime hours, and a third list for Holidays. When you enable (activate) an ACL, the currently enabled (active) ACL is automatically disabled (de-activated). In other words, there can only be one active ACL.

The only restriction on the amount of ACLs you can create is that the total number of rules cannot exceed 512. So, you could create a single ACL with 512 rules; or one ACL with 300 rules and a second with 212 rules, etc.... See the section Creating Access Lists for guidelines to consider when designing ACLs.

An ACL name can be a number. For example, you can create a list whose name is 1 or 151. If you chose to use numbers, keep in mind the following restrictions:

- Numbers 1 through 99 are reserved for Standard type Rules ***ONLY***. So, for example, if you try to create an Extended Rule whose ACL Name is 1, it will be rejected.
- Numbers 100 through 199 are reserved for Extended type Rules ***ONLY.*** So, for example, if you try to create a Standard Rule whose ACL Name is 100, it will be rejected.
- ACL names that contain any letter (Alphabetic) character, can be either Standard or Extended.
- You cannot mix ACL types in a list. This means that if you create an ACL with a Standard Rule with ACL Name Test1, you cannot create an Extended Rule in ACL Test1. If you do, you will receive the following message:

  ```
  Access Rule Name is already being used by the
  other type.
  Choose a different name and try again
  ```

## How Packets are Processed

Assuming an ACL is active, when a packet arrives on the Avaya Multiservice switch, the parameters in the packet are compared to the parameters in the Access Rule starting with the lowest index number. If there is a match, that rule is applied to the packet and the search stops.

If the 5-tuple's of the packet and rule do not match, the next (higher index) rule is compared. This process continues until a match is found, or there are no more rules. There is an implied **permit all** at the end of every list. Therefore, if no match is found, the packet is forwarded with the priority un-changed.

## What are Wildcards?

Wildcards are a template that govern which part of an IP address is significant when evaluating a rule. When you create a rule based on source or destination IP address, you must also specify the Wildcard.

Wildcards are in principal, the same as a subnet mask. The differences are you invert the mask's bits and there is no requirement of contiguous bits. For Example: a decimal wildcard of 0.255.0.255 is allowed.

For example: If you want to create a rule that blocks all traffic on the 192.168.24.0 (subnet mask 255.255.255.0) network, you would specify a Wildcard of 0.0.0.255 in the rule.

If you wanted to block traffic from a specific host whose IP address was 192.168.24.143 (subnet mask 255.255.255.0) you would specify a Wildcard of 0.0.0.0. This mask "tells" the supervisor to evaluate the entire IP address when evaluating a packet against the rule.

## What is TCP Established?

TCP Established is a criteria applied by a rule where the "Acknowledge" bit in a TCP header is examined. If this option is not "checked", the rule will apply to the packets whose Acknowledge bit is clear (0). If the option is checked, packets that have the Acknowledge bit set will be affected by the rule.

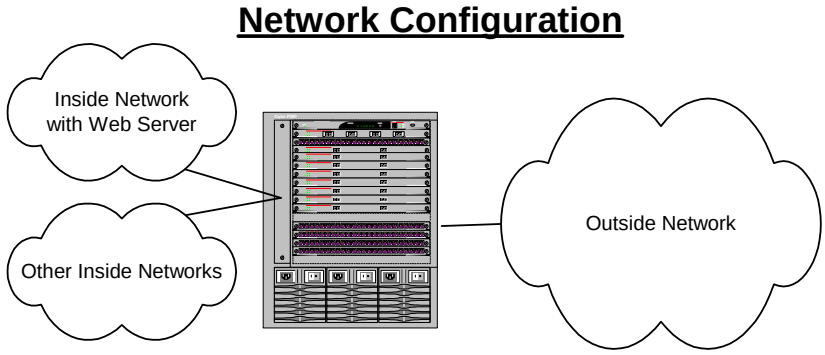
The Acknowledge bit in the TCP header, when 0, indicates that the packet is an initial "call" to the destination. The host sending the message will clear the bit (0). The host that responds to the message will set the bit(1) indicating this message is a response. Effectively the call is now "Established". All subsequent packets between these two hosts for this session will have the Acknowledge bit set.

For example: Suppose the Avaya Multiservice switch has interfaces to "Outside" networks as well as interfaces to "Inside" networks. The

Outside networks need access to a web server and should be denied access to any other resource within the Inside network.

Hosts on the Inside networks should have full access to all other resources on the Inside.

The Web server itself should not be able to establish any new connections to the Outside but should be able to pass traffic to the other Inside networks




Assume the following abbreviations:

WS = Web Server.
IN = Inside Networks
ON = Outside Networks
Any = Both Inside and Outside Networks

The rules for implementing the above restrictions would be as follows:

***Table 6-16.***

| Rule # | Rule | TCP Established |
|---|---|---|
| 1 | allow Any to call WS dest port 80 | Un-Checked |
| 2 | allow WS to respond | Checked |
| 3 | allow WS to IN | Un-Checked |
| 4 | deny WS to Any (Outside) | Un-Checked |
| 5 | allow IN to Any | Un-Checked |
| 6 | deny remaining traffic from Outside to Any | Un-Checked |

Rules 1 and 2 collectively manage ***web*** traffic ***to and from*** the web server (WS). Rule 1 says that any source address can get to the web server's IP address using destination port 80. Because the TCP Established criteria is unchecked, hosts from any network can send a TCP "call setup" message as a first step in requesting a web page.

Rule 2 says that the web server may respond to any (TCP) web request. Although it can send a message back to **any** address from any source port, only messages that are in response to a web request will be forwarded because TCP Established is checked and the source port criteria is specified.

Rules 3 and 4 handle traffic from the web server that is not in response to a web request. Rule 3 gives the web server access to the rest of the Inside networks. And Rule 4 blocks the web server from getting to the rest of the networks (Outside).

Rule 5 gives the hosts on the Inside network access to any network.

Rule 6 blocks any other host from using resources on any of the Inside networks.

*** Note:** In this simple example, pseudo-rules are used. In practice, the pseudo-rule "allow WS to IN" would require that you create rules that forward traffic from the web server's IP address to ***each*** network on the Inside explicitly. If you had 30 inside networks, you'd create 30 rules. This is where a subnetted network would be powerful; because you could summarize subnets into a few rules.

# Creating Access Lists

## Creating Standard Access Rules

To create standard access rules:

1. Select **Access Lists** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Access List** dialog box opens (Figure 6-30).

   *** Note:** The IP Access List displays all standard and extended access rules that have been created. If no rules have been created, the following statement displays: No IP Access Rules are currently configured.

   Due to its size, Figure 6-30 shows the Access List dialog box split in two separate sections.

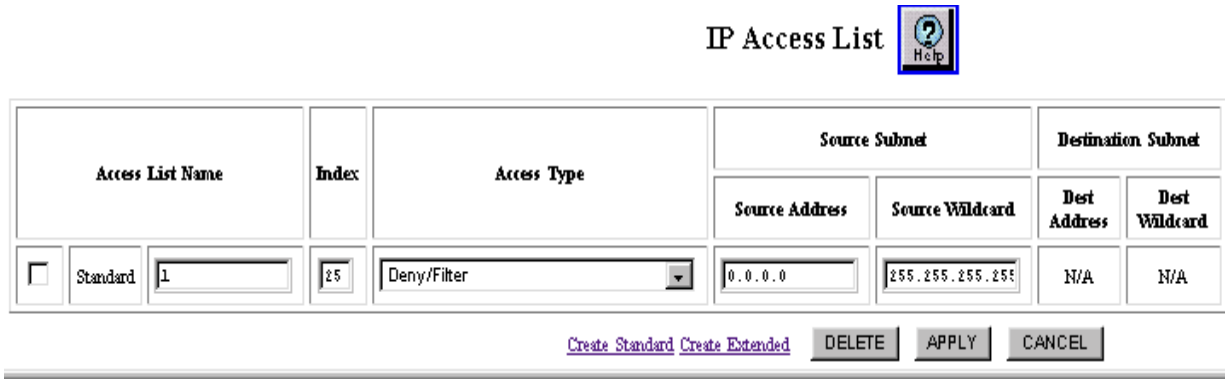
The switch supports a maximum total of 512 access control rules, regardless of the number of access lists. For example, you could create the following three ACLs:

- ACL A with 100 rules
- ACL B with 200 rules
- ACL C with 212 rules

The combined total of rules cannot exceed 512. Only one access control list can be enabled at a time.

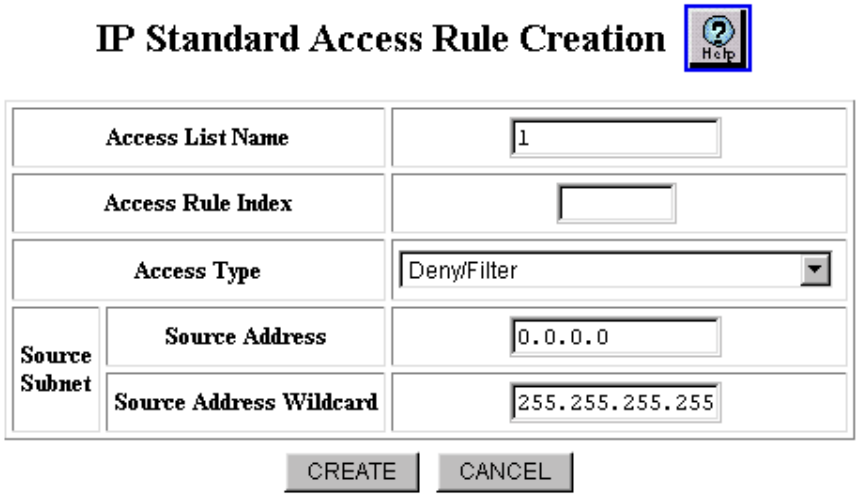
Index numbers of access rules can range from 1 to 512. Do not use index numbers higher than 512.

***Figure 6-30. IP Access List Dialog Box***



2. Click **Create Standard**. The **Create Standard Access List** dialog box opens (Figure 6-31).

***Figure 6-31. Create IP Standard Access List Dialog Box***




3. Refer to Table 6-17 to configure the **Create Standard IP Access List** dialog box to filter or prioritize traffic:

***Table 6-17. Create Standard IP Access List Dialog Box Parameters***

| Parameter | Allows you to... |
|---|---|
| **Access List Name** | The Avaya Multiservice switch supports ACL names up to 32 characters (Alpha-Numeric). Spaces are allowed in the names but are not recommended. Instead of spaces, use the underscore "_" character.<br>Refer to "Naming Conventions for ACLs" on page 18 for more information |
| **Access Rule Index** | Enter the sequence number for each new rule you create. Index numbers can be 1 through 512. Packets are compared against rules in ascending index order.<br>**Note:** Entering a new rule may override other rules. Review your current configuration prior to creating new access list rules. |

*Table 6-17. Create Standard IP Access List Dialog Box Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **Access Type** | Select the method of handling incoming datagrams based on the IP access type from the following pull-down menu options:<br>• **Deny/Filter** - Allows you to filter out (drop) packets based on the specified configuration.<br>• **Permit/Fwd pri8 (high) to pri1 (low)** - Allows you to prioritize traffic based on the specified configuration.<br>• **Permit/Fwd with no change in priority** - Allows you to forward traffic with no change in priority. |
| **Source Subnet** | • **Source Address** - Enter the IP address that you want to deny or grant access to the switch. The Wildcard will determine how the address is evaluated.<br>• **Source Address Wildcard** - Enter the Wildcard for this address. See the section "What are Wildcards?" on page 19 for more information on Wildcards. |

4. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

## Creating Extended Access Rules

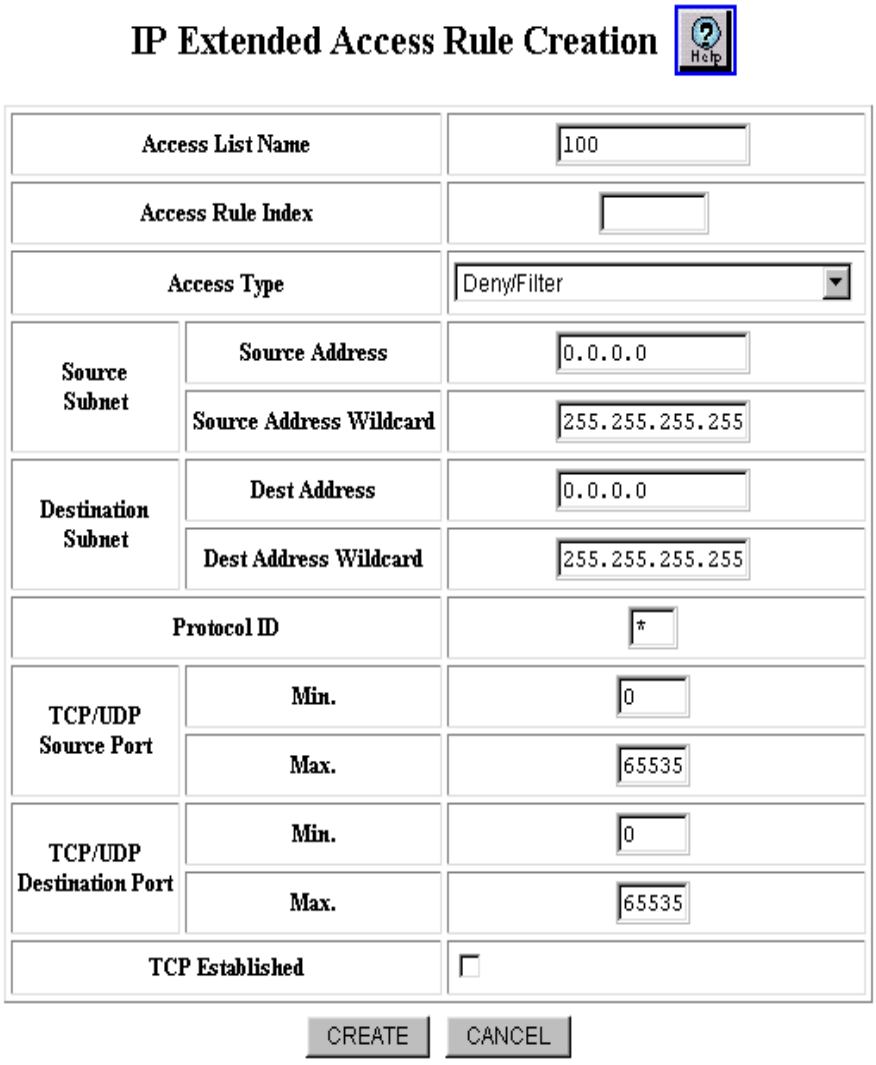
To create Extended Access Rules:

1. Select **Access Lists** from the **Routing > IP >Configuration** group on the Web Agent window. The **IP Access List** dialog box opens (Figure 6-30).

   *** Note:** The **IP Access List** dialog box displays all standard and extended access rules that have been created. If no rules have been created, the following statement displays: No IP Access Rules are currently configured.

2. Select **Create Extended**. The **IP Extended Access Rule Creation** dialog box opens (Figure 6-32).

*Figure 6-32. IP Extended Access Rule Creation Dialog Box*



3. Refer to Table 6-18 to configure the **IP Extended Access Rule Creation** dialog box parameters to filter or prioritize traffic:

*Table 6-18. IP Extended Access Rule Creation Parameters*

| Parameter | Allows you to... |
|---|---|
| **Access List Name** | Enter the alphanumeric name of the access list this rule will be added to. Refer to "Naming Conventions for ACLs" on page 18 for more information |
| **Access Rule Index** | Enter the sequence number for each new rule you create. Index numbers can be 1 through 512. Packets are compared against rules in ascending index order.<br>**Note:** Entering a new rule may override other rules. Review your current configuration prior to creating new access list rules: |
| **Access Type** | Select the method of handling incoming datagrams based on the IP access type you set from the following options:<br>• **Deny/Filter** - Allows you to filter out traffic based on the specified configuration.<br>• **Permit/Fwd pri8 (high) to pri1 (low)** - Allows you to prioritize traffic based on the specified configuration.<br>• **Permit/Fwd with no change in priority** - Allows you to forward traffic with no change in priority. |
| **Source Subnet** | • **Source Address** - Enter the IP address that you want to deny or grant access to the switch. The Wildcard will determine how the address is evaluated.<br>• **Source Address Wildcard** - Enter the Wildcard for this address. See the section "What are Wildcards?" on page 19 for more information on Wildcards. |
| **Destination Subnet** | • **Dest Address** - Enter the IP address that you want to deny or grant access to the switch. The Wildcard will determine how the address is evaluated.<br>• **Dest Address Wildcard** - Enter the Wildcard for this address. See the section "What are Wildcards?" on page 19 for more information on Wildcards. |
| **Protocol ID** | Specify a protocol ID to be filtered. (For example, ICMP=1, IGMP=2). A single asterisk (*) indicates all protocols.<br>RFC 1700 defines the protocol IDs.<br>To see the complete list of protocol numbers, refer to the URL:<br>http://www.isi.edu/in-notes/iana/assignments/protocol-numbers |

*Table 6-18. IP Extended Access Rule Creation Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **TCP/UDP Source Port** | Specify a range of source ports that pass between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). Options include:<br>• **Min.** - The lowest numbered port in the range. The default is 0.<br>• **Max.** - The highest numbered port in the range. The default is 65,535.<br>*** Note:** The protocol ID parameter must first be configured with either 6 for TCP or 17 for UDP, to enable the TCP/UDP Source port parameter.<br>To see the complete list of well-known port numbers (specifically in relation to the destination port), refer to the URL:http://www.iana.org/assignments/port-numbers |
| **TCP/UDP Destination Port** | Specify a range of destination ports that pass data between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). Options include:<br>• **Min.** - The lowest numbered port in the range. The default is 0.<br>• **Max.** - The highest numbered port in the range. The default is 65,535.<br>*** Note:** The protocol ID parameter must first be configured with either 6 for TCP or 17 for UDP, to enable the TCP/UDP Destination port parameter.<br>To see the complete list of well-known port numbers (specifically in relation to the destination port), refer to the URL:http://www.isi.edu/in-notes/iana/assignments/port-numbers |
| **TCP Established** | Criteria for matching TCP packets of established (connected) or not established (initial call) sessions. |

4. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

# Activating Access Lists

You can activate access lists on the switch through the Web Agent and the CLI.

## Activating Access Lists Using the Web Agent

To activate an access list using the Web Agent:

*** Note:** Before you can activate an access list, you must first configure the access lists. For information about configuring access lists, refer to "Access Lists (also called Access Control Lists or ACLs)" earlier in this chapter.

1. Select **Access Control** from the **Routing > IP > Configuration** group on the Web Agent. The **IP Access Control** dialog box opens (Figure 9-10).

***Figure 6-33. IP Access Control Dialog Box***

2. Select **Enable** from the **Enable** field pull-down menu to filter inbound traffic.
3. Select the name of the access list to be used for filtering when IP access control is enabled from the **IP Access List** field pull-down menu.
4. Click **APPLY** to save your changes.

## Activating Access Lists Using the CLI

To activate an access list using the CLI, enter the following command in configure mode:

```
<configure># access-group <access-list-name>
```

To disable an access list using the CLI command, enter the following command in configuration mode:

```
<configure># no access-group <access-list-name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

## Example: Filtering Web Traffic Using an Access Rule

To configure your switch to filter web traffic to a particular web server:

1. Select **Access Lists** from the **Routing > IP > Configuration** group on the Web Agent window. The IP Access List dialog box displays (Figure 6-30).
2. Select **Create Extende**d. The **IP Extended Access Rule Creation** dialog box displays (Figure 6-32).
3. Enter a number between 100 and 199 (or Alphanumeric) (for extended ACL) in the **Access List Name** field to identify your new access control list.
4. Enter a number in the **Access Rule Index** field to identify the access rule.
5. Select **Deny/Filter** from the **Access Type** field pull-down menu.
6. Leave 0.0.0.0 and 255.255.255.255 as the Source Address and Source Address Wildcard for the Source Subnet parameter settings. All source traffic will match.
7. Enter the IP address in the **Dest Address** field that represents the destination address of the web server. Enter a wildcard of 0.0.0.0 to identify the specific IP address of the destination web server.

*** Note:** To deny/filter traffic to a specific address and not to an entire subnet, you must specify the destination IP address of the network node, and use a subnet wildcard of 0.0.0.0.

8. Specify the TCP protocol ID = 6. If you specify TCP or UDP port numbers, you must specify Protocol ID 6 or 17 respectively.
9. Enter the following in the **TCP/UDP Destination Port** field:

— a Min. of 80 (HTTP).

— a Max. of 80 (HTTP).

10. Leave the **TCP/UDP Source Port** field alone:

— a Min. of 0 (HTTP).

— a Max. of 65536 (HTTP).

11. Select **TCP Established**. A check mark displays in the check box.

12. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

Each time any end user attempts to access the web server specified by the destination TCP/UDP ports, all web requests are filtered.

## Second Example

Filtering Traffic Between 10.1.1.0 and 10.1.2.0 Subnets. It is possible to filter traffic to either a specific address or to an entire subnet. In this example, all traffic between the two subnets is filtered:

This example also assumes that the network is a Class C sub network (255.255.255.0).

To filter traffic between both subnets, you must create two access rules.

To create the Extended Access list and rules:

1. Select **Access Lists** from the **Routing > IP > Configuration** group on the web Agent window. The **IP Access List** dialog box opens (Figure 6-30).

2. Select **Create Extended**. The **IP Extended Access Rule Creation** dialog box opens (Figure 6-32).

3. Enter a number between 100 and 199 (or Alphanumeric) (extended ACL) in the **Access List Name** field to identify your new access control list.

4. Enter a number in the **Access Rule Index** file to identify the access rule.

5. Select **Deny/Filter** from the **Access Type** field pull-down menu.

6. Enter the source address (10.1.2.0) and the source address wildcard (0.0.0.255), respectively, in the **Source Address** field.

7. Enter the destination address (10.1.1.0) and the destination address wildcard (0.0.0.255), respectively, in the **Dest Address** field.

8. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings. Once you create both access rules, all traffic between subnet 10.1.1.0 and 10.1.2.0 is deny/filtered.

*** Note:** Traffic between any other 10.1.x.0 subnets are not filtered because the access rules only deny/filter traffic between subnets 10.1.1.0 and 10.1.2.0.

To deny/filter traffic to a specific address and not to an entire subnet, you must specify the destination IP address of the network node, and use a subnet wildcard of 0.0.0.0.

To deny/filter all traffic, you must specify a destination address of 0.0.0.0 and a wildcard of 255.255.255.255. This is useful if you want to filter all traffic except traffic that matches a previous rule. Ensure that you *do not* make this your first rule, since ACL rules are read from the top down and stop after the first rule match, which ignores all subsequent rules.

# Optimizing Performance when Using an Access Control List

*** Note:** This section provides a detailed discussion of the architecture and functionality of the Avaya Multiservice switch with respect to ACLs. This material goes well beyond standard configuration issues by addressing system performance, memory management and optimization.

## Purpose

The purpose of this section is to explain the configuration options when using Access Lists. Deploying an Access List affects the use of hardware and software resources and may impact system performance. An Access Control List (ACL), also referred to as an Access List, is a tool for associating rules (permit, deny, prioritize for Quality of Service (QoS)) with identified IP traffic through the switch. This section will show how to monitor performance and adjust configurations to optimize performance.

## Important Terms used in this section

The following terms are used extensively in this section:

- **5-tuple**: The five elements that fully describe the criteria of the ACL rule: Source IP/ Mask, Destination IP/Mask, Protocol, Source Port, Destination Port. The masks allow the user to specify a narrow or wide range of matches. All elements are optional, but the Ports are only valid if TCP or UDP is the selected protocol and can be expressed as a single port or range of ports. The protocol ID for TCP and UDP is 6 and 17 respectively.
- **Access List/Access Control List** (ACL): an ordered list of ACL Rules.
- **ACL Rule**: An element of an ACL that identifies traffic based upon a 5-tuple (condition), and specifies a queue (0-7), permit, or deny action for packets matching the condition.
- **CPU**: The general processor for the P580/P882 that resides on the Supervisor module. The CPU determines whether to forward or filter packets. It identifies Flows by resolving IP-to-MAC addressing and matching ACL Rules. It updates the F-chip's forwarding cache for future Fast Path'ing of packets that match this Flow. The process of examining Flows and updating all of the F-chips' forwarding caches is called Slow Path.
- **DA:** Destination IP Address.
- **F-chip**: Forwarding-chip (F-chip) is an application specific integrated circuit (ASIC) that forwards recognized packets via Fast Path or unrecognized packets via Slow Path. It learns or flushes L3 forwarding entries (L3FE) as directed by the CPU. In earlier versions of the hardware, the F-Chip was referred to as the Packet Routing Engine (PRE).
- **Fast Path**: When an F-chip is able to recognize and forward a packet to the destination port without CPU intervention. Both FIRE (media modules) and FORE (supervisor module) are Fast Path forwarding mechanisms.
- **FIRE (Fast In-Band Routing Engine):** When an 80-series Ethernet media module has been licensed for routing, the F-Chips on that module provide fast, direct forwarding of L3 packets to their destination ports. The destination ports can be on the same module or a different module.
- **Flow**: A set of routed packets that get the same Layer 3 Forwarding Entry (L3FE) due to equivalent address characteristics. The complexity of this equivalence will affect the frequency that packets match a single Flow. In the

simplest case, such as no ACL present, a Flow is identified only by the destination address of the packet, for a high rate of L3FE re-use. In the most complex case, such as an ACL that specifies the entire 5-tuple, the granularity of identification will cause a very low rate of re-use.

- **FORE (Fast Out-of-Band Routing Engine):** When an 80-series Ethernet media module is not licensed for routing, the media modules forward all routed packets to the supervisor. The F-Chip on the supervisor module provides fast, direct forwarding of L3 packets to their destination ports.
- **Hash Mode:** The F-chip uses a 12-bit key to initially locate available memory for Flows. In DA-only mode (default) it builds the key from a sample of the Flow's destination address (DA). In SA-DA mode, it uses both the source and destination addresses. The F-chip automatically selects which 12 bits to use, and when to re-hash with a different key.
- **Ingress F-chip:** The F-chip that receives a packet from an external source.
- **Layer 3 Forwarding Entry (L3FE)**: When a packet arrives on a media module, the F-Chip needs to know where to forward that packet. The L3 forwarding cache is a list that identifies the path taken by a data packet through the switch. Each entry in this list is a L3FE. Each entry is identified by a combination of the Flow's 5-tuple and the corresponding ACL rule. If the F-chip does not find a match in the L3 forwarding cache, the packet is sent Slow Path to the CPU for processing and forwarding. Once the CPU has determined the destination, it updates the L3 forwarding cache on the F-chips with the L3FE. Once updated, the F-chip can forward future packets via Fast Path.
- **SA:** Source IP Address.
- **Slow Path**: When an ingress F-chip does not recognize a packet compared to its cache of known Flows, the packet is forwarded to the CPU to determine proper destination and ACL Rule assignment. See Layer 3 Forwarding Entry.

## How to Optimize Performance when using ACLs

There are several techniques to optimize performance. They are related and must be considered together.

- Recognize Performance Issues
- Evaluate System Performance

- Enable Routing at the Module
- Design Safe, Efficient ACLs
- Identify the Ports
- Configure Hash Mode
- Manage F-Chip memory
- Manage Cache Timers

## Recognize Performance Issues

When the ACL is the root of a performance problem, it shows as the Slow Path becoming overused. The Slow Path is not designed to handle significant traffic levels since the single CPU also handles all other management functions. There are several ways to determine if the CPU is overloaded:

- Continuous PING to the supervisor: timeouts or inconsistent timing of echo responses.
- Slow Scrolling LED Marquee: This is good visual sign that the CPU is busy.
- Slow Management response: If Avaya Multiservice Network Manager (MSNM), Avaya Policy Manager (APM), HPOV, or a MIB browser get slow updates, this can signify a busy CPU or saturated network.
- Slow network response: This can be measured in a variety of ways.

Once you have determined that the ACL is the root cause, and have optimized the rules, you need to tune system parameters.

# Evaluate System Performance

The first step is to determine whether the use of an ACL affects system performance. This requires an analysis of traffic patterns, the use of device statistics, and a "process of elimination". If you suspect that the use of an ACL is degrading system performance and "Disabling Access Control" improves performance, you are ready to begin the process.

In order to perform the diagnosis, you need to generally identify routed Flows through the switch. You will need this information to match Flows against the F-chip statistics to locate the problem area.

The next step (and this will be repeated as needed) is to note the usage statistics with and without the ACL enabled.

## Slow Path versus Fast Path

The goal is to maximize Fast Path traffic (L3 Frame Cache Hits) and minimize Slow Path traffic (L3 Slow Path Frames). The easiest parameters to monitor are found on the Forwarding Statistics web page found on the switch Web Agent by selecting the following:

**Routing>L3 Forwarding Cache> Forwarding Statistics**

The Forwarding Statistics web page shows the breakdown of traffic by FIRE Fabric port/Chip Index (see below).

**Frame Forwarding Statistics**

| Select | FIRE Fabric Port/Chip Index | L3 Total | L3 Frame Cache Hits | Percent Cache Hits | L3 Slow Path Frames | Percent Slow Path | L3 Drop Frames | Percent Drops | RX Frame Count (T2) | L2 Frame Count (T2) |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1/1 | 5,325,825 | 5,010,778 | 94% | 315,047 | 5% | 0 | 0% | n/a | n/a |
| ☐ | 4/1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% | n/a | n/a |
| ☐ | 5/1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% | n/a | n/a |
| ☐ | 32/1 | 43,798 | 14,438 | 32% | 29,360 | 67% | 0 | 0% | n/a | n/a |

CLEAR REFRESH

## How Many Cache Entries?

Each F-chip/PRE (see Identify the Ports section below for PRE column explanation) reserves space for IP Unicast, IP multicast, and IPX. By default, the number of entries are limited to 15,000 for each (45,000 total). If the CPU attempts to add an entry in excess of 15,000, the L3FE will not be stored and that Flow will only be forwarded via the Slow Path. When looking at the Active FE

Cache(Cache Contents) page, the **Current Entries** column indicates how many entries are currently in the L3F cache. Since the L3 forwarding cache is recalculated periodically, you need to monitor the FE Cache web page on the switch Web Agent found by selecting the following:

**Routing>L3 Forwarding Cache>Cache Contents**

Layer 3 forwarding entries live for a time that is the maximum of two timers:

- The *Age Interval* for entries in the layer 3 forwarding cache (The default setting is 120 seconds. You can set this timer to a value from 120 to 360 seconds.)

  The Age interval timer starts when a new forwarding entry is added to the layer 3 forwarding cache. Each forwarding entry has its own timer.

- The *chassis timer* for layer 3 forwarding entries. This timer is an internal timer that you cannot change. The setting for this timer is dependent on the number and type of modules (number of F-Chips) in the chassis.

  The chassis timer specifies the number of seconds that the CPU takes to rebuild all forwarding caches on all F-chips in the chassis. Each second, the CPU removes expired forwarding entries from one protocol branch (IP-UNI, IP-Multi, or IPX) of the forwarding cache on one F-Chip and then rebuilds the branch.

  On a fully populated P882, rebuilding all forwarding caches on all F-chips takes 400 seconds. On a fully populated P580, this task takes 160 seconds.

The FE Cache page displays as shown below.

**Active FE Cache**

| Select | Fabric/Chip Index | Type | Mode | Memory Use in Bytes | Total Entries | Current Entries | Aged Entries | Duplicate Add Attempts | Failed Add Attempts | Entries Removed due to Route Deletes | Entries Removed due to Route Changes | Lookup Hits | Lookup Misses | Lookup Levels |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1/1 | IP_UNI | DA-Only | 134 | 389 | 1 | 387 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| ☐ | 1/1 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 1/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/1 | IP_UNI | DA-Only | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| ☐ | 4/1 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 5/1 | IP_UNI | DA-Only | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| ☐ | 5/1 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 5/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 32/1 | IP_UNI | DA-Only | 0 | 3 | 0 | 2 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| ☐ | 32/1 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 32/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Clear | Refresh | Flush Entry | Flush Table

## Enable Routing at the Module

The P580/P882 has the option of centralized (unlicensed) or distributed (licensed) routing function. When a module is licensed, the on-board F-Chips (FIRE) provide the Fastpath processing. When a module is unlicensed, the Fastpath is handled by the single F-Chip (FORE) on the Supervisor Module. Since the presence of an ACL will consume more F-Chip memory, it is recommended to license all modules in a chassis. This distributes the work load among more resources.

## Design Safe, Efficient ACLs

The entry of ACL rules via the CLI, web or Avaya Policy Manager does not encourage or enforce any checking beyond correct syntax. The general guideline is that you are configuring a Layer-3 switch,

not a firewall! The following are some criteria for designing safe, efficient ACLs and how they affect performance:

- **Specify Destination Address:** The wildcard feature of rule creation is a convenience but can explode the number of identified Flows. Since the “standard” ACL implies “any” for the destination, it should also be used with care. It is desirable for the wildcard to match a specific set of addresses.
- **Use Protocols/Ports Carefully:** By pushing the ACL-to-packet matching up one or two levels of the IP stack, it refines the granularity of the Flows to be very specific in what is matched. A source-port range can cause a large number of “micro” Flows to be created.
- **Minimize Rules:** The number of rules has a direct impact on the CPU effort to match rules to Flows. This is especially true when there is a high frequency of packets that are “walked down” the entire list and don’t match any rules.
- **Minimize Searching:** The goal is to place the most frequently matched rules toward the beginning of the ACL. This requires a good knowledge of traffic patterns. This can be noticeable as ACLs get longer.
- **Permit Management Traffic with High Priority:** This include routing updates (unicast for RIP 1, multicast for RIP 2), SNMP (CajunView, HPOV), LDAP (for Cajun Rules/Avaya Policy Manager). Not doing this can cause loss of management connectivity.

# Identify the Ports

The chassis is organized by slots, fabric ports, PRE/F-chip's, and physical ports. The number of F-Chips and physical ports vary with the module type. This information is useful in spreading the workload evenly among resources, and identifying possible choke points:

- Every Fabric port can manage up to 4 F-Chips
- Slot 1 has 1 Fabric port only
- Slots 2-7 (P580) and Slots 2-17 (P882) have 2 Fabric ports per slot
- The Supervisor has 1 F-chip (FORE)
- The 8-port GigE has 8 F-Chips (4 per Fabric port)
- The 4-port GigE has 4 F-Chips (2 per Fabric port)
- The 24-port Ethernet modules (copper or fiber) have 2 F-Chips (1 per Fabric port). Physical Ports 1-12 correspond with F-Chip 1, and Physical Ports 13-24 correspond with F-Chip 2.
- The 48-port Ethernet has 4 F-Chips (2 per Fabric port) with the following Physical Port to F-Chip correspondence: ports 1-12: F-Chip 1, ports 13-24: F-Chip 2, ports 25-36: F-Chip 3, ports 37-48: F-Chip 4.

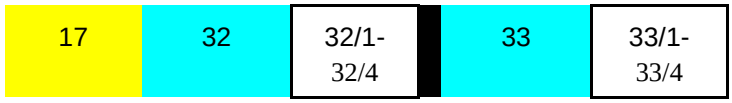
Fabric ports are numbered regardless of whether other slots are empty or full.

For switch code version 5.3.1, F-Chips numbers are associated with their respective Fabric ports. To locate the Fabric port and F-Chip for Physical Port you need to know the media type and slot.

For example, Physical port 20 on a 24 port Ethernet module that is in slot 4 of the chassis is identified by Fabric Port 7 and F-Chip 2. This will be displayed as Chip 7/2. These absolute addresses are not affected by the placement/type of other modules.

**Fabric and F-Chip Assignments**

| Slot | Fabric Port | F-Chip(s) | Fabric Port | F-Chip(s) | Comments |
|---|---|---|---|---|---|
| 1 | 1 | 1 | | | Supervisor has 1 F-Chip |
| 2 | 2 | 2/1-2/4 | 3 | 3/1-3/4 | |
| 3 | 4 | 4/1-4/4 | 5 | 5/1-5/4 | |
| 4 | 6 | 6/1-6/4 | 7 | 7/1-7/4 | |
| 5 | 8 | 8/1-8/4 | 9 | 9/1-9/4 | |
| 6 | 10 | 10/1-10/4 | 11 | 11/1-11/4 | |
| 7 | 12 | 12/1-12/4 | 13 | 13/1-13/4 | Last slot of a P580 |
| | | | | | |
| 8 | 14 | 14/1-14/4 | 15 | 15/1-15/4 | |
| 9 | 16 | 16/1-16/4 | 17 | 17/1-17/4 | |
| 10 | 18 | 18/1-18/4 | 19 | 19/1-19/4 | |
| 11 | 20 | 20/1-20/4 | 21 | 21/1-21/4 | |
| 12 | 22 | 22/1-22/4 | 23 | 23/1-23/4 | |
| 13 | 24 | 24/1-24/4 | 25 | 25/1-25/4 | |
| 14 | 26 | 26/1-26/4 | 27 | 27/1-27/4 | |
| 15 | 28 | 28/1-28/4 | 29 | 29/1-29/4 | |
| 16 | 30 | 30/1-30/4 | 31 | 31/1-31/4 | |




# Configuring Hash Mode

If your diagnosis shows a performance degradation with an ACL enabled, the IP Unicast Hash mode needs to be changed from "DA-only" to "SA-DA".

To do this from the switch Web Agent, select:
**Routing>L3 Forwarding Cache> Cache Configuration> IP Unicast Hash Mode**
To do this from the switch CLI, enter the following command in Configure mode:

**<configure># ip unicast route-cache hash-mode sa-da**

This can cause a noticeable increase in the total Flows identified resulting in a increased F-chip memory usage. See the next section in this case.

**Important**: Changing the Hash Mode parameter affects every L3-enabled F-chip on the P580/P882.

# Managing F-chip Memory

The reconfiguration of Hash Mode can cause a secondary effect: increased cache usage. By default, the IP Unicast Cache size is 15000 entries per F-chip. Although this can be used up simply due to a high number of Flows (e.g., a proxy server for the internet), the SA-DA Hash Mode will always cause more Flows to be identified than in the DA-only mode.

The F-chip memory can accommodate approximately 70,000 total entries for routed (L3) Flows. This is comprised of IP Unicast, IP Multicast, and IPX entries for that F-chip. The running total is viewable via the Web Agent as follows:

For the CPU L3, select:
**Routing>L3 Forwarding Cache>Cache Configuration> Current System Entries**

For each F-chip, select:
**Routing>L3 Forwarding Cache>Cache Contents,**

**Active FE Cache**

| Select | Fabric/Chip Index | Type | Mode | Memory Use in Bytes | Total Entries | Current Entries | Aged Entries | Duplicate Add Attempts | Failed Add Attempts | Entries Removed due to Route Deletes | Entries Removed due to Route Changes | Lookup Hits | Lookup Misses | Lookup Levels |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1/1 | IP_UNI | DA-Only | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 1/1 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 1/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/1 | IP_UNI | DA-Only | 118724 | 1584877 | 886 | 1583990 | 37465 | 0 | 0 | 0 | 0 | 0 | 28 |
| ☐ | 4/1 | IP_MUL | SA-DA | 952 | 3430 | 7 | 2597 | 654 | 0 | 826 | 0 | 0 | 0 | 7 |
| ☐ | 4/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/2 | IP_UNI | DA-Only | 0 | 2583 | 0 | 2582 | 29 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/2 | IP_MUL | SA-DA | 0 | 8 | 0 | 8 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/2 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/3 | IP_UNI | DA-Only | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/3 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/3 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/4 | IP_UNI | DA-Only | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/4 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 4/4 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 5/1 | IP_UNI | DA-Only | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 5/1 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 5/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

As long as these totals stay under 70K, it is safe to increase the IP Unicast Maximum Entries to prevent overflow. If the switch is not routing IPX or has minimal IP Multicast traffic, it is generally safe to double the IP Unicast maximum to 30000.

You can do this from either the switch Web Agent or the switch CLI.

To double the IP Unicast maximum to 30000 from the Web Agent, select:

**Routing>L3 Forwarding Cache>Cache Configuration> IP Unicast Maximum Entries >**

To double the IP Unicast maximum to 30000 from the CLI, enter the following CLI command in Configure mode:

```
<configure># ip unicast route-cache max-size 30000
```

**Important:** Changing the Maximum Cache Entries parameter affects every L3-enabled F-chip on the P580/P882.

## Creating IP Static Routes

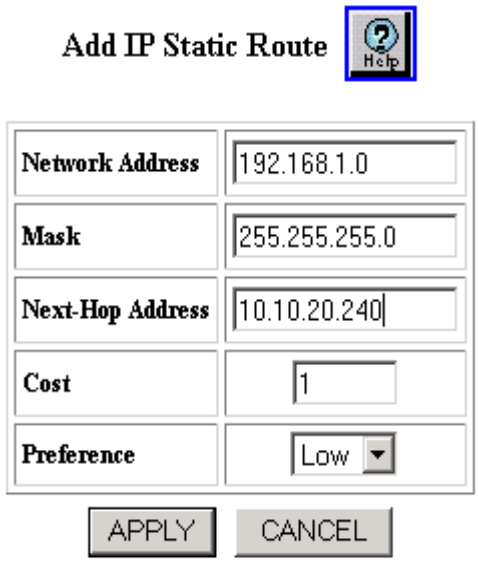
You can create IP static routes using either the Web Agent or the CLI.

## Creating IP Static Routes Using the Web Agent

To create IP static routes using the Web Agent:

1. Select **Static Routes** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Static Routes** dialog box opens (Figure 9-10).

*Figure 6-34. Add IP Static Route dialog box*




2. Refer to Table 6-19 to configure the **IP Static Route** dialog box parameters:

*Table 6-19. IP Static Route Parameters*

| Parameter | Allows you to... |
|---|---|
| **Network Address** | Enter an IP network address for your IP static route. |
| **Mask** | Enter an IP subnet mask for your IP static route. |
| **Next-Hop Address** | Enter an IP address for the gateway associated with the IP static route. |
| **Cost** | Enter the metric between this router and the destination. |
| **Preference** | Select a *low* or *high* routing preference from the Preference field pull-down menu. |

3. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

### Using the CLI

To create and show IP static routes using the CLI in configure mode:

```
<configure># ip route <ip-addr> <mask> <next hop
IP address> <cost> <preference>
<configure># show ip route static
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

## Creating IP Static ARP Entries

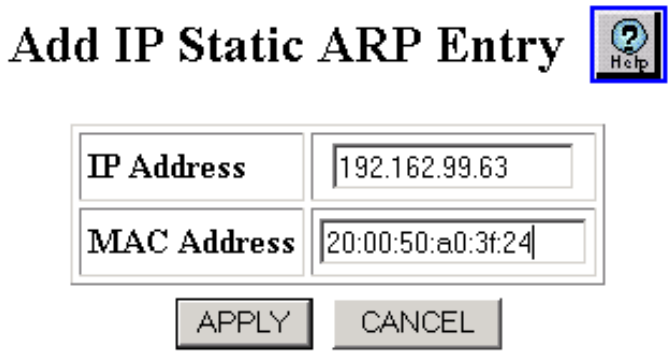
You can create static ARP entries on the switch using the Web Agent or the CLI.

### Creating IP Static ARP Entries Using the Web Agent

To create a static ARP entry in your switch's ARP cache using the Web Agent:

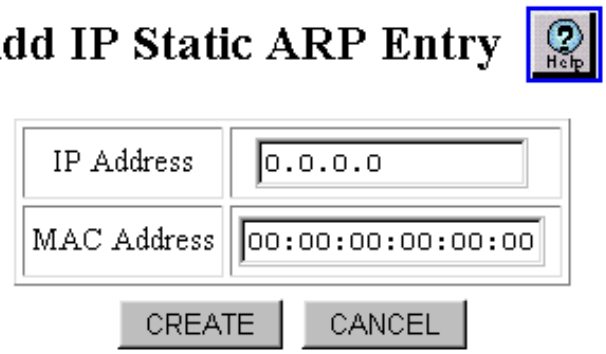
1. Select **Static ARP** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Static ARP Entries** dialog box opens (Figure 6-35).

***Figure 6-35. IP Static ARP Entries Dialog Box***




2. Select **CREATE**. The **Add IP Static ARP Entry** dialog box opens (Figure 9-12).

***Figure 6-36. Add IP Static ARP Entry Dialog Box***




3. Refer to Table 6-20 to configure the **Add IP Static ARP Entry** dialog box parameters:

***Table 6-20. IP Static ARP Parameters***

| Parameter | Allows you to... |
|---|---|
| **IP Address** | Enter an IP address to associate with the Static ARP entry. |
| **MAC Address** | Enter the MAC address of a node to which you want to create a static ARP entry. |

4. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

### Creating IP Static ARP Entries Using the CLI

To create IP static ARP entries using the CLI, enter the following command in Configure mode:

```
<configure># arp <ip-address> <hardware-address>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

## Creating a BOOTP/DHCP Server Entry

The BOOTP/DHCP Server Entry allows you to configure a Router as a BOOTP/DHCP Relay Agent between a BOOTP/DHCP server and the requesting client.

You can create a BOOTP/DHCP Server entry using either the Web Agent or the CLI.

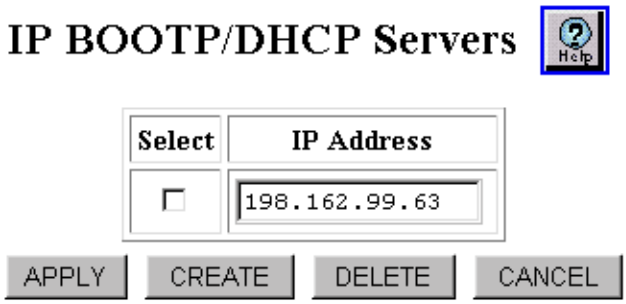
*** Note:** BootP/DHCP must first be enabled in the **IP Global Configuration.**

## Creating a BOOTP/DHCP Server Entry Using the Web Agent

To create a BOOTP/DHCP entry using the Web Agent:

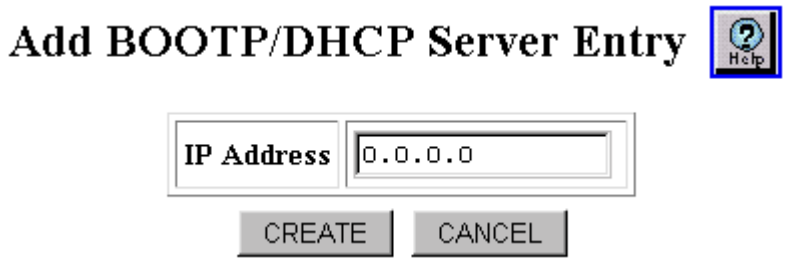
1. Select **BOOTP/DHCP Servers** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP BOOTP/DHCP Servers** dialog box opens (seeFigure 6-37).

*Figure 6-37. IP BOOTP/DHCP Server Dialog Box*




2. Select **CREATE**. The **Add BOOTP/DHCP Server Entry** dialog box opens (Figure 9-14).

*Figure 6-38. Add BOOTP/DHCP Server Entry Dialog Box*




3. Enter the BOOTP/DHCP server IP address in the **IP Address** field.

4. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

*** Note:** It is possible to create multiple BOOTP/DHCP Server Entries if necessary.

## Creating a BOOTP/DHCP Server Entry Using the CLI

To create a BOOTP/DHCP entry using the CLI, enter the following command in Configure mode:

```
<configure># ip boot-dhcp server
<ip-address>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Option 82 for DHCP

Option 82 for DHCP includes two options:

- **Circuit Info**, identifies the slot and physical port number from which the DHCP request was received.
- **Agent Info**, identifies the IP address and, if available, the system name of the switch.

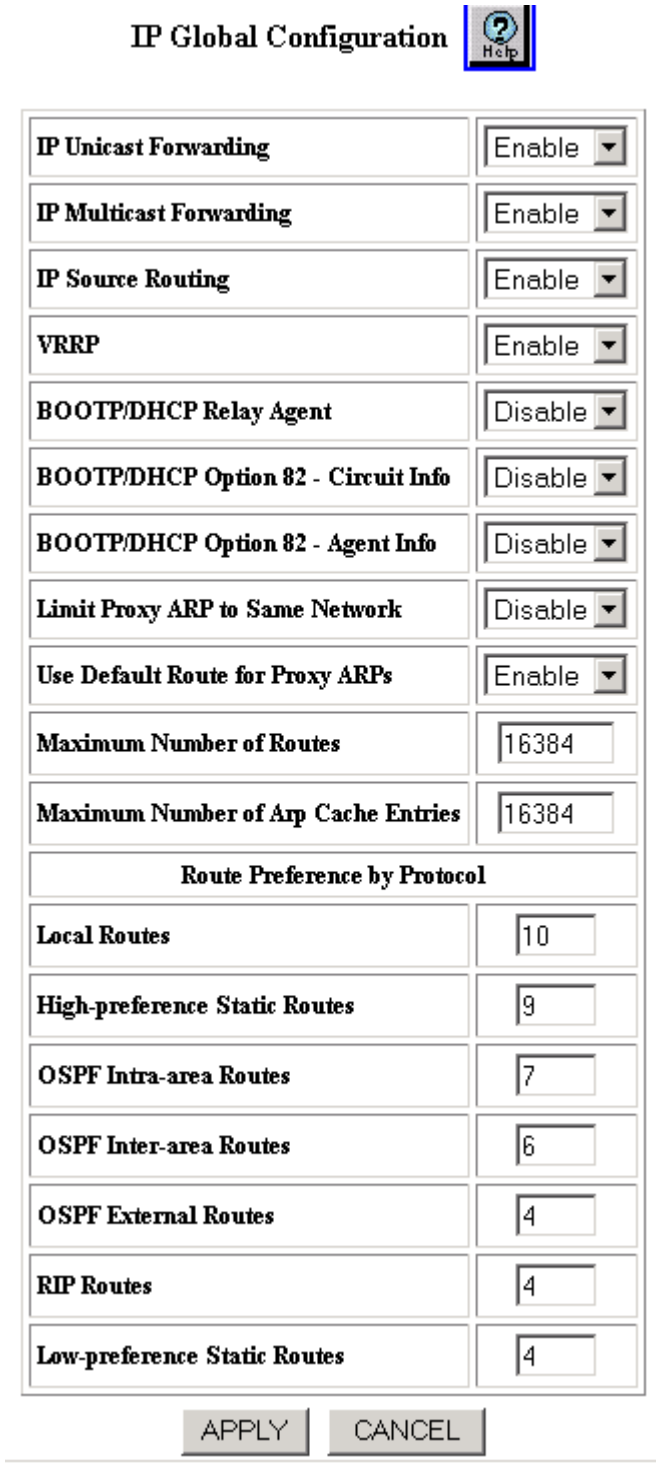
By default, both of these suboptions are disabled. You can enable either or both suboptions by using the Web Agent or the CLI.

## Enabling Option 82 by Using the Web Agent

To use the Web Agent to change the status of option 82:

1. Select **Global** from the **Routing >IP > Configuration** group. The **IP Global Configuration** dialog box opens (Figure 6-39).

*Figure 6-39. IP Global Configuration Dialog Box*




2. Open the pull-down menus from the **DHCP Option - Circuit Info** and **DHCP Option 82 - Agent Info** fields.

3. Select **Enable**.

*** Note:** BOOTP/DHCP relay Agent must be set to enable, and must be enabled on the desired IP interface (enabled by default).

### Enabling Option 82 by Using the CLI

To use the CLI to enable Option 82, enter Global Configuration mode and use the following commands:

- To enable circuit info 1, use the following command:

  **<configure># ip bootp-dhcp circuit-info**

- To enable agent info 2, use the following command:

  **<configure># ip bootp-dhcp agent-info**

- To disable circuit info 1, use the following command:

  **<configure># no ip bootpdhcp circuit-info**

- To disable agent info 2, use the following command:

  **<configure># no ip bootp-dhcp agent-info**

For detailed information on how to enter Global Configuration command mode, see "Accessing/Exiting the Command Modes" in Chapter 1, "*Overview*," of the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* .

# IP Multicast

IP Multicast enables a single host to distribute information to multiple recipients. To do this, multicast protocols use class D IP addresses to specify specific multicast groups to which information is sent. The class D IP address used by multicast routing protocols, ranges from 224.0.0.1 to 224.0.0.255. The class D IP addresses available for general use are 224.0.1.0 to 239.255.255.255.

In addition, IP multicasting distributes information to multicast groups in two specific ways:

- **Multicast Forwarding** - allows a switch to forward multicast traffic from the local multicast server to group members on directly attached subnetworks. If a multicast packet is forwarded to multiple interfaces on one VLAN, only one Forwarding Entry is added on the VLAN for the packet.

One copy of the packet is sent to the VLAN.To configure interfaces for multicast forwarding select Internet Group Management Protocol (IGMP) for the multicast protocol.

*** Note:** Interfaces configured for IGMP forwarding will not be able to participate in multicast sessions distributed through DVMRP Routing.

- **Multicast Routing** - allows a switch to deliver multicast traffic between neighboring routers and across the network using Distance Vector Multicast Routing Protocol (DVMRP).To configure interfaces for multicast routing select DVMRP for multicast protocol on all interfaces that are part of a multicast network.Since IGMP is required on all interfaces that have multicast clients, IGMP is enabled automatically on all interfaces configured for DVMRP.

*** Note:** You must globally enable IP multicast routing in order to successfully configure IGMP or DVMRP. Refer to "Routing Function," earlier in this chapter, for instructions on enabling IP multicast routing.

## Configuring IGMP

IGMP enables hosts to inform routers when they join or leave groups. Routers periodically query hosts (query interval) for the groups in which the hosts are members. When there is more than one router in a broadcast domain (subnet), one of the routers becomes the designated querier. Only the designated router queries the hosts.

Both IGMP Version 1.0 and IGMP Version 2.0 are supported. After selecting the specific IGMP version for an interface, you can manually configure the Version 1.0 querier. The selection of the querier for Version 2.0 is dynamic but can be overridden.

Configuring IGMP includes enabling IGMP and the MTRACE globally on the switch. You can do this from either the Web Agent or the CLI.

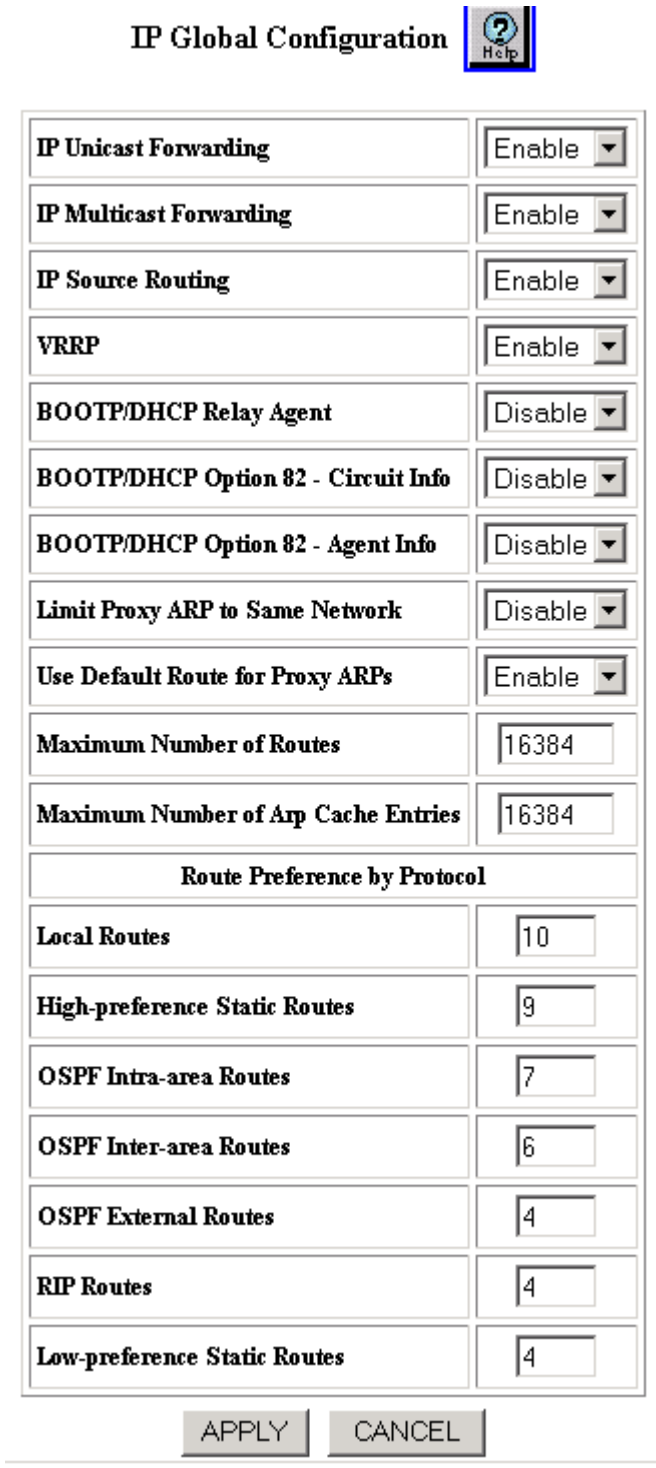
*** Note:** You also have to enable multicast forwarding from the Routing > IP > Configuration > Global

## Globally Enabling IGMP Using the Web Agent

To globally enable IGMP from the Web Agent:

1. Select **Global Configuration** from the **Routing > IP > Configuration** group in the Web Agent window. The **IP Global Configuration** dialog box opens (Figure 9-15).

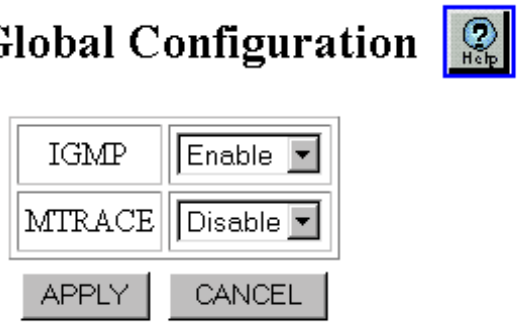
***Figure 6-40. IP Global Configuration Dialog Box***




2. Select **Enable** from the **IP Multicast Forwarding** field pull-down menu to enable IP multicast globally.

3. Select **Global Configuration** from the **Routing > IGMP** group on the Web Agent window. The **IGMP Global Configuration** dialog box opens (Figure 6-41).

*Figure 6-41. IGMP Global Configuration Dialog Box*




4. Select **Enable** from the **IGMP** field pull-down menu to enable IGMP.
5. Select **Enable** from the **MTRACE** field pull-down menu to enable MTRACE processing.
6. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Globally Enabling IGMP Using the CLI

To globally enable IGMP using the CLI, enter the following command from Configure mode:

```
<configure># set router igmp
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

## Modifying IGMP Interfaces Using the Web Agent

To modify IGMP interfaces from the Web Agent:

1. Select **Interfaces** from the **Routing > IGMP** group on the Web Agent window. The **IGMP Interfaces** dialog box opens (Figure 9-18)

   *** Note:** You must first enable "multicast protocol"on an interface before you can configure IGMP. Refer to *"Displaying Existing IP Interfaces"* earlier in this chapter for more information on how to select a multicast protocol.

***Figure 6-42. IGMP Interfaces Dialog Box***

IGMP Interfaces

| Select | Interface | IP Address | IP Address Mask | IGMP Version | Maximum Groups | Always Be Group Membership Querier | Process Leave Packets | Query Request Interval in (sec) | Query Response Interval in (sec) | Neighbor Querier Timeout Interval in (sec) | Robustness Variable |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 13 | 10.0.1.129 | 255.255.255.128 | v2 | 32 | Disable | Enable | 125 | 10 | 255 | 2 |
| ☐ | vlan_10.0.3.1_jwiebe | 10.0.3.1 | 255.255.255.128 | v2 | 32 | Disable | Enable | 125 | 10 | 255 | 2 |
| ☐ | 18 | 10.0.4.1 | 255.255.255.128 | v2 | 32 | Disable | Enable | 125 | 10 | 255 | 2 |
| ☐ | 22 | 10.0.6.1 | 255.255.255.128 | v2 | 32 | Disable | Enable | 125 | 10 | 255 | 2 |
| ☐ | 23 | 10.0.6.129 | 255.255.255.128 | v2 | 32 | Disable | Enable | 125 | 10 | 255 | 2 |
| ☐ | 50 | 192.168.50.100 | 255.255.255.0 | v2 | 32 | Disable | Enable | 125 | 10 | 255 | 2 |
| ☐ | Inet_inband | 10.0.7.1 | 255.255.255.128 | v2 | 32 | Disable | Enable | 125 | 10 | 255 | 2 |

APPLY CANCEL

2. Refer to Table 6-21 to modify an IGMP interface:

***Table 6-21. IGMP Interface Parameters***

| Parameter | Allows you to... |
|---|---|
| **Select** | Select the interface to be modified. |
| **Interface** | Displays the IP interface that is configured with IGMP. |
| **IP Address** | Displays the IP address associated with this interface.<br>**Note:** This parameter is not configurable from the IGMP configuration dialog box. |
| **IP Address Mask** | Displays the subnet mask associated with this interface.<br>**Note:** This parameter is not configurable from the IGMP configuration dialog box. |

*Table 6-21. IGMP Interface Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **IGMP Version** | Select the IGMP Version (1.0 or 2.0) to be associated with the IGMP interface. |
| **Maximum Groups** | Enter the number of IGMP Groups that can be active on this interface. The default value is 32. |
| **Always be Group Membership Querier** | **Version 1.0** - Select **Enable** to make this interface the designated querier. The default is **Disable**.<br>**Version 2.0** - Select **Enable** to force this interface to send queries. The default is **Disable** which tells the interface to obey the designated querier election.<br>**Note:** Only the designated router will query hosts on your network. |
| **Process Leave Packets** | turns off processing of IGMP leave messages when set to disable. The default value is **Enable**. |
| **Query Request Interval in (sec)** | Enter a time period between queries. The default value is **125** seconds. |
| **Query Response Interval in (sec)** | Enter a time (in seconds) to wait for a response from a host after a query is sent. If no response is received within this time, the host is removed from the group table. The default value is **10** seconds. |
| **Neighbor Querier Timeout Interval in (sec)** | Enter a time (in seconds) this interface should wait after hearing a neighbor's query before assuming the role of querier, if not already the querier. If no query is received from a neighbor with a lower IP address in the allotted time, this interface becomes the querier (IGMP Version 2.0 only). The default value is **255** seconds. |
| **Robustness Variable** | Modify this field for any expected packet loss on a subnet. If a subnet is expected to have more packet loss, the Robustness Variable should be increased. The Robustness Variable *must not* be set to 0 and *should not* be set to 1. The default value is **2**. |

3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Modifying IGMP Interfaces Using the CLI

To modify an IGMP interface using the CLI, enter the following command from interface mode:

```
(config-if:<interface>)# ip igmp <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Configuring and Modifying Distance Vector Multicast Routing Protocol (DVMRP)

DVMRP uses IP packets with protocol type 2 (IGMP) to exchange routing datagrams. DVMRP enables multicast routers to exchange distance vector updates that contain multicast flow lists and their corresponding cost metrics. DVMRP may use tunneling between pairs of DVMRP routers when traffic must pass through one or more intermediary routers or gateways that do not implement DVMRP.This implementation adheres to the specification for DVMRP V3.

You can configure DVMRP Globally using either the Web Agent or the CLI.

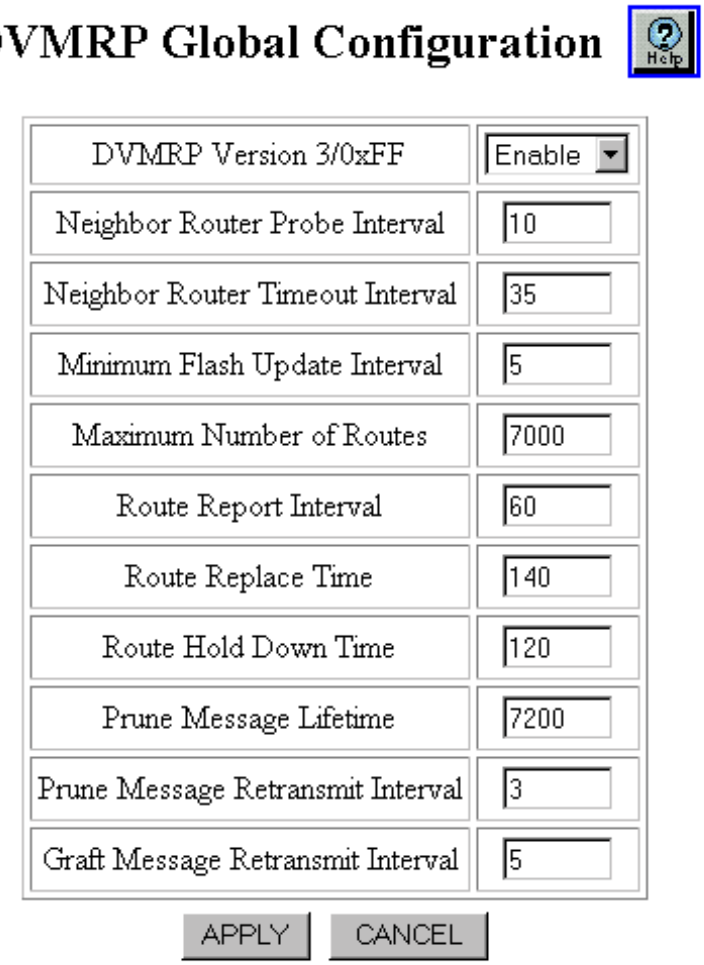
*** Note:** When processing heavy traffic, the switch may lose a small number of DVMRP neighbor-to-neighbor probe messages. The loss of these messages may cause multicast routing to become unstable.

## Configuring the DVMRP Global Configuration Using the Web Agent

To configure DVMRP globally using the Web Agent:

1. Select **Global Configuration** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Global Configuration** dialog box opens (Figure 6-41).
2. Select **Enable** from the I**P Multicast Forwarding** field pull-down menu to enable IP multicast globally.
3. Select **Global Configuration** from the **Routing > DVMRP** group on the Web Agent window. The **DVMRP Global Configuration** dialog box opens (Figure 9-19).

*Figure 6-43. DVMRP Global Configuration Dialog Box*




4. Select **Enable** from the **DVMRP Version 3/0xFF** field pull-down menu.

5. Refer to Table 6-22 to configure the **DVMRP Global Configuration** dialog box parameters:

*Table 6-22. DVMRP Global Configuration Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **DVMRP Version 3/xFF** | Select **Disable** to globally disable DVMRP. The default value is **Enable**. |
| **Neighbor Router Probe Interval** | Enter **probe interval** (in seconds) for the switch to probe the network for available neighbor routers. |
| **Neighbor Router Timeout Interval** | Enter the **time-out interval** (in seconds) that a neighbor stays up without confirmation. This is an important method used to time-out old routes. |

*Table 6-22. DVMRP Global Configuration Dialog Box Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **Minimum Flash Update Interval** | Enter the **update interval** (in seconds) between flash updates. This represents the minimum time between advertisements of the same route. |
| **Maximum Number of Routes** | Enter the maximum number of routes for this interface. |
| **Route Report Interval** | Enter the **report interval** (in seconds) that elapses between delivery of DVMRP routing table updates. |
| **Route Replace Time** | Enter the amount of **replace time** (in seconds) before which a route entry will be removed if it is not refreshed. |
| **Route Hold Down Time** | Set the **hold down time** (in seconds) that the switch reports unavailable routes with a metric of infinity. |
| **Prune Message Lifetime** | Enter the **lifetime** (in seconds) that a transmitted upstream prune message persists. |
| **Prune Message Retransmit Interval** | Enter the **retransmit interval** (in seconds) between the transmittal of generated upstream prune messages on your network. |
| **Graft Message Retransmit Interval** | Enter the **retransmit interval** (in seconds) between the transmittal of generated upstream graft messages. |

6. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Configuring the DVMRP Global Configuration Using the CLI

To configure DVMRP globally using the CLI:

```
<configure># router dvmrp
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

## Modifying a DVMRP Interface

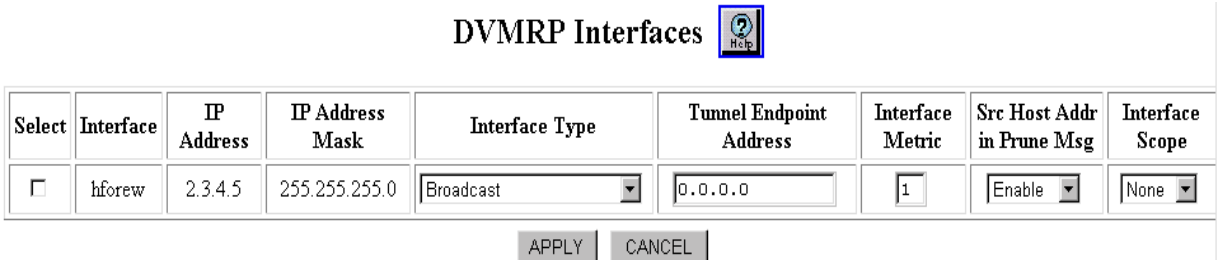
You can modify a DVMRP interface using either the Web Agent or the CLI.

### Modifying the DVMRP Interface Using the Web Agent

To modify a DMVRP interface using the Web Agent:

1. Select **Interfaces** from the **Routing > DVMRP** group of the Web Agent window. The **DVMRP Interfaces** dialog box opens (see Figure 6-44).

*Figure 6-44. DVMRP Interfaces Dialog Box*




*** Note:** You must first set "multicast protocol" on an interface to DVMRP before you can configure DVMRP. Refer to *"Displaying Existing IP Interfaces"*, earlier in this chapter, and enable a multicast protocol for this interface.

**2.** Refer to Table 6-23 to complete your DVMRP configuration:

*Table 6-23. DVMRP Interface Parameters*

| Parameter | Defines the... |
|---|---|
| **Select** | Select a DVMRP interface that you want to configure. |
| **Interface** | Displays the Interface that is configured with the DVMRP multicast protocol. |
| **IP Address** | Displays the IP address of each interface. You cannot modify this field. |
| **IP Address Mask** | Displays the Subnet mask for each interface. You cannot modify this field. |
| **Interface Type** | Select an Interface type. You can configure the interface type as:<br>• **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation.<br>• **Non-Encapsulated Tunnel** - All multicast data traffic is IPIP encapsulated, but the protocol messages are unicast.<br>• **IPIP Tunnel** - All multicast traffic (data and protocol messages) are encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP). |
| **Tunnel Endpoint Address** | Displays the Tunnel endpoint IP address of a router. You can modify this setting to represent the end router IP address to which you want to send datagrams through a tunnel. The origin and endpoint routers are separated by a gateway(s) or a router(s) that do not support DVMRP. |
| **Interface Metric** | Displays the Cost metric for the interface. |

*Table 6-23. DVMRP Interface Parameters continued*

| Parameter | Defines the... |
|---|---|
| **Src Host Addr in Prune Msg** | Select **Disable to s**end prune messages with only the subnet portion of the source address.<br>The default is **Enable (**sends prune messages with the full source host address). |
| **Interface Scope** | Select the minimum TTL (time-to-live) required for a packet to leave this interface. The options are None, 127, and 255. |

3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Modifying the DVMRP Interface Using the CLI

To configure the DVMRP Interface using the CLI:

```
(configure-if:<interface># ip dvmrp <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Monitoring Switch Performance Using IP Statistics

This section provides detailed information on the analysis and use of IP and IP multicast statistics.

IP routing statistic options include:

- Displaying Global IP Routing Statistics using the Web Agent
- Searching the IP Routing Table
- Displaying the IP Routing Table Statistics
- Searching the IP ARP Cache

# Displaying Global IP Routing Statistics

You can monitor switch performance using either the Web Agent or the CLI.

## Displaying Global IP Routing Statistics Using the Web Agent

To display the global IP routing statistics using the Web Agent:

*** Note:** IP routing global statistics only represent traffic processed by the supervisor module software.

1. Select **Global Statistics** from the **Routing > IP > Display** group on the Web Agent window. The **IP Routing Global** Statistics dialog box opens (see Figure 6-45)Shown in two figures.

***Figure 6-45. IP Routing Global Statistics Dialog Box***

IP Global Statistics

| | | | |
|---|---|---|---|
| **IP In Receives** | 71555 | **IP In Header Errors** | 0 |
| **IP In Address Errors** | 0 | **IP Forward Datagrams** | 275 |
| **IP In Unknown Protocols** | 0 | **IP In Discards** | 0 |
| **IP In Delivers** | 68606 | **IP Out Requests** | 55079 |
| **IP Out Discards** | 0 | **IP Out No Routes** | 0 |
| **IP Reassembly Timeout Period** | 60 | **IP Reassembly Required** | 0 |
| **IP Reassembly OKs** | 0 | **IP Reassembly Failures** | 0 |
| **IP Fragmentation OKs** | 0 | **IP Fragmentation Failures** | 0 |
| **IP Fragmentation Creates** | 0 | **IP Routing Discards** | 0 |
| **ICMP In Messages** | 0 | **ICMP In Errors** | 0 |
| **ICMP In Destination Unreachables** | 0 | **ICMP In Time Exceeds** | 0 |
| **ICMP In Parameter Problems** | 0 | **ICMP In Source Quenchs** | 0 |
| **ICMP In Redirects** | 0 | **ICMP In Echo Requests** | 0 |
| **ICMP In Echo Replies** | 0 | **ICMP In Timestamp Requests** | 0 |

2. Click

| | | | |
|---|---|---|---|
| ICMP In Timestamp Replies | 0 | ICMP In Address Mask Requests | 0 |
| ICMP In Address Mask Replies | 0 | ICMP Out Messages | 0 |
| ICMP Out Errors | 0 | ICMP Out Destination Unreachables | 0 |
| ICMP Out Time Exceededs | 0 | ICMP Out Parameter Problems | 0 |
| ICMP Out Source Quenches | 0 | ICMP Out Redirects | 0 |
| ICMP Out Echo Requests | 0 | ICMP Out Echo Replies | 0 |
| ICMP Out Timestamp Requests | 0 | ICMP Out Timestamp Replies | 0 |
| ICMP Out Address Mask Requests | 0 | ICMP Out Address Mask Replies | 0 |
| UDP In Datagrams | 2856 | UDP In No Ports | 0 |
| UDP In Errors | 0 | UDP Out Datagrams | 0 |
| IP Multicast Forward Datagrams | 0 | IP Multicast In Discards | 0 |
| IP Multicast In Receives | 0 | | |
| BOOTP/DHCP In Requests | 0 | BOOTP/DHCP In Responses | 0 |
| BOOTP/DHCP In Discards | 0 | BOOTP/DHCP In Hops Exceededs | 0 |
| BOOTP/DHCP Out Requests | 0 | BOOTP/DHCP Out Responses | 0 |

CLEAR REFRESH

**a.** **Clear** to set all statistics to zero.

**b.** **Refresh** to update all statistics.

**3.** Refer to Table 6-24 to review the definition of each statistic:

***Table 6-24. IP Routing Global Statistics***

| Statistic | Defines the... |
|---|---|
| **IP In Receives** | Total number of input datagrams received from interfaces, including those received in error. |
| **IP In Header Errors** | Number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options. |

*Table 6-24. IP Routing Global Statistics continued*

| Statistic | Defines the... |
|---|---|
| **IP In Address Errors** | Number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| **IP Forward Datagrams** | Number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.<br>**Note:** This is routed by the supervisor in the software. |
| **IP In Unknown Protocols** | Number of input datagrams discarded due to errors in their IP headers. Such errors may include bad checksums, version number mismatches, other format errors, time-to-live exceeded, errors discovered in processing their IP options. |
| **IP In Discards** | Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space).<br>**Note:** This counter does not include any datagrams discarded while awaiting re-assembly. |
| **IP In Delivers** | Total number of input datagrams successfully delivered to IP user-protocols (including ICMP). |
| **IP Out Requests** | Total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission.<br>**Note:** This counter does not include any datagrams counted in ipForwDatagrams. |

*Table 6-24. IP Routing Global Statistics continued*

| Statistic | Defines the... |
|---|---|
| **IP Out Discards** | Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but were discarded (for example, for lack of buffer space). Note that this counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion. |
| **IP Out No Routes** | Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any Datagrams which a host cannot route because all of its default gateways are down. |
| **IP Reassembly Timeout Period** | Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity. |
| **IP Reassembly Required** | Number of IP fragments received that need to be reassembled. |
| **IP Reassembly OKs** | Number of IP datagrams successfully reassembled. |
| **IP Reassembly Failures** | Number of failures detected by the IP re-assembly algorithm (timeout errors). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received. |
| **IP Fragmentation OKs** | Number of IP datagrams that have been successfully fragmented at this entity. |
| **IP Fragmentation Failures** | Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be. |
| **IP Fragmentation Creates** | Number of IP datagram fragments that have been generated as a result of fragmentation at this entity. |
| **IP Routing Discards** | Number of routing entries that were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries. |

*Table 6-24. IP Routing Global Statistics continued*

| Statistic | Defines the... |
|---|---|
| **ICMP In Messages** | Total number of ICMP messages that the entity received. Note that this counter includes all those counted by icmpInErrors. |
| **ICMP In Errors** | Number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length). |
| **ICMP In Destination Unreachables** | Number of ICMP Destination Unreachable messages received. |
| **ICMP In Time Exceeds** | Number of ICMP Time Exceeded messages received. |
| **ICMP In Parameter Problems** | Number of ICMP Parameter Problem messages received. |
| **ICMP In Source Quenchs** | Number of ICMP Source Quench messages received. |
| **ICMP In Redirects** | Number of ICMP Redirect messages received. |
| **ICMP In Echo Requests** | Number of ICMP Echo (request) messages received. |
| **ICMP In Echo Replies** | Number of ICMP Echo Reply messages received. |
| **ICMP In Timestamp Requests** | Number of ICMP Timestamp (request) messages received. |
| **ICMP In Timestamp Replies** | Number of ICMP Timestamp Reply messages received. |
| **ICMP In Address Mask Requests** | Number of ICMP Address Mask Request messages received. |
| **ICMP In Address Mask Replies** | Number of ICMP Address Mask Reply messages received. |
| **ICMP Out Messages** | Total number of ICMP messages that this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors. |
| **ICMP Out Errors** | Number of ICMP messages that this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations, there may be no types of error which contribute to this counter's value. |
| **ICMP Out Destination Unreachables** | Number of ICMP Destination Unreachable messages sent. |
| **ICMP Out Time Exceeds** | Number of ICMP Time Exceeded messages sent. |

*Table 6-24. IP Routing Global Statistics continued*

| Statistic | Defines the... |
|---|---|
| **ICMP Out Parameter Problems** | Number of ICMP Parameter Problem messages sent. |
| **ICMP Out Source Quenchs** | Number of ICMP Source Quench messages sent. |
| **ICMP Out Redirects** | Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects. |
| **ICMP Out Echo Requests** | Number of ICMP Echo (request) messages sent. |
| **ICMP Out Echo Replies** | Number of ICMP Echo Reply messages sent. |
| **ICMP Out Timestamp Requests** | Number of ICMP Timestamp (request) messages sent. |
| **ICMP Out Timestamp Replies** | Number of ICMP Timestamp Reply messages sent. |
| **ICMP Out Address Mask Requests** | Number of ICMP Address Mask Request messages sent. |
| **ICMP Out Address Mask Replies** | Number of ICMP Address Mask Reply messages sent. |
| **UDP In Datagrams** | Total number of UDP datagrams delivered to User Datagram Protocol (UDP) users. |
| **UDP In No Ports** | Total number of received UDP datagrams for which there was no application at the destination port. |
| **UDP In Errors** | Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. |
| **UDP Out Datagrams** | Total number of UDP datagrams sent from this entity. |
| **IP Multicast Forward Datagrams** | Number of input multicast datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. |
| **IP Multicast In Discard** | Number of input IP multicast datagrams for which no problems were encountered to prevent their continued processing, but were discarded (for example, for lack of buffer space).<br>**Note:** This counter does not include any datagrams discarded while awaiting re-assembly. |

*Table 6-24. IP Routing Global Statistics continued*

| Statistic | Defines the... |
|---|---|
| **IP Multicast In Receives** | Total number of input multicast datagrams received from interfaces, including those received in error. |
| **BOOTP/DHCP In Requests** | Number of requests received by the BOOTP/ DHCP Relay Agent. |
| **BOOTP/DHCP In Responses** | Total number of BOOTP/DHCP response datagrams received by the BOOTP/DHCP Relay Agent. |
| **BOOTP/DHCP In Discards** | Number of BOOTP/DHCP requests discarded.Incremented when an IP interface receives a DHCP/BootP request, but the IP interface does not have the BooTP/DHCP Relay Gateway Enabled. |
| **BOOTP/DHCP In Hops Exceeds** | Number of BOOTP/DHCP requests not forwarded due to number of hops exceeds. |
| **BOOTP/DHCP Out Requests** | Total number of BOOTP/DHCP requests forwarded by the BOOTP/DHCP Relay Agent. |
| **BOOTP/DHCP Out Responses** | Total number of BOOTP/DHCP responses forwarded by the BOOTP/DHCP Relay Agent. |

## Displaying Global IP Routing Statistics Using the CLI

To display the global IP routing statistics using the CLI, enter the following command from the enable mode or configuration mode prompt:

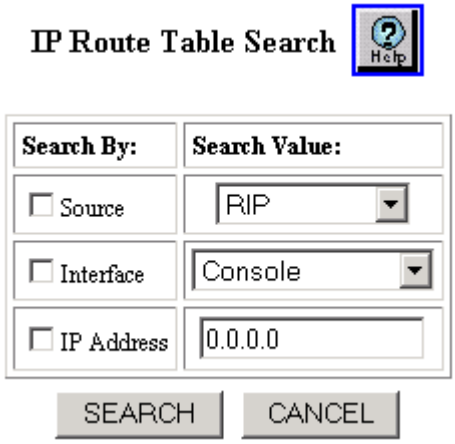
```
>#  show ip traffic
```

## Searching the IP Routing Table

To use the IP routing table:

1. Select **Route Table Search** from the **Routing > IP > Display** group on the Web Agent window. The **IP Route Table Search** dialog box opens (Figure 6-46).

*Figure 6-46. IP Route Table Search Dialog Box*




2. Select the search criteria you want to use to find more specific information on available routes. For example, if you want to find all static routes that are presently configured on your switch, search by *source* and specify *static* as your search value.

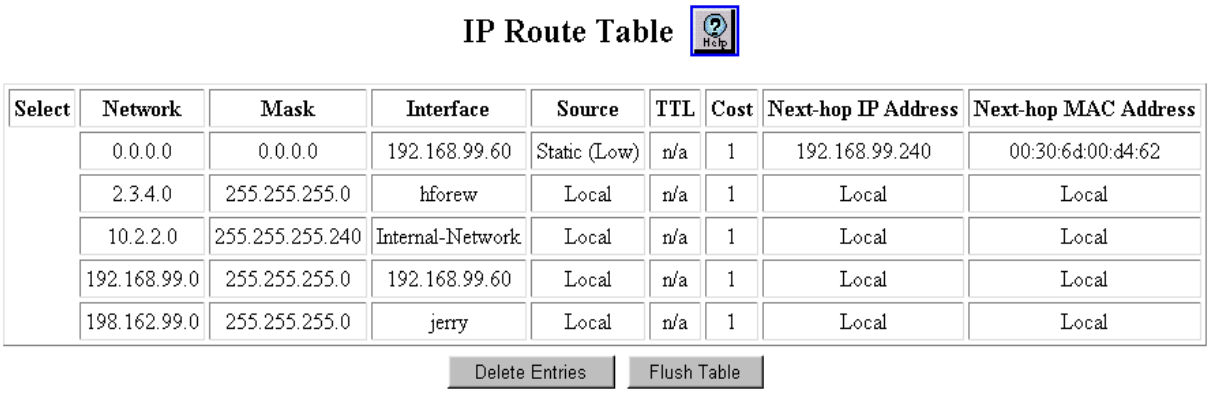
3. Refer to Table 6-25 to determine your search parameters:

***Table 6-25. IP Route Table Search Parameters***

| Parameter | Allows you to search... |
|---|---|
| **Source** | Your IP routing table using one of the following parameters:<br>• RIP<br>• OSPF<br>• Static<br>• Local<br>Once you select one of these parameters, the search attempts to find routes associated with that parameter. |
| **Interface** | The interface you selected. System default entries include:<br>• **Default**<br>• **Discard**<br>• Ethernet Console<br>• Configured Interface |
| **IP Address** | The IP address you entered. |

4. Select **SEARCH**. If routes are available, they are displayed in the **IP Routing Table** dialog box (Figure 6-47).

*Figure 6-47. IP Route Table Dialog Box*



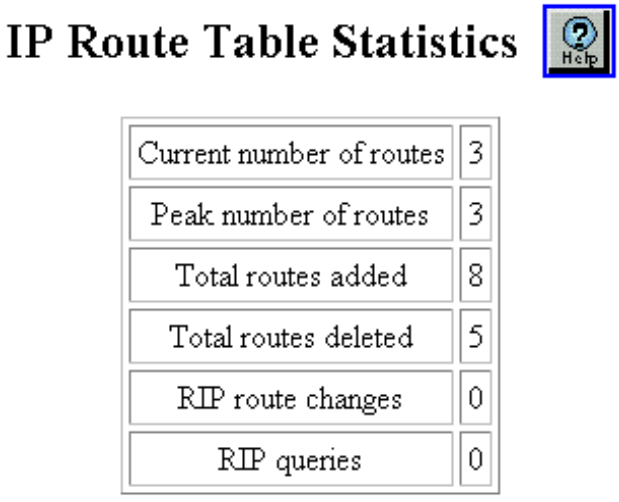

*** Note:** To delete a local entry from your IP routing table, you must delete the local IP interface associated with that entry.

## Displaying the IP Routing Table Statistics

To display the IP Routing Table Statistics:

1. Select **Route Table Statistics** from the Ro**uting > IP > Display** group on the Web Agent window. The **IP Routing Table Statistics** dialog box opens (Figure 6-48)

*Figure 6-48. IP Route Table Statistics Dialog Box*



## Displaying Global IP Routing Statistics Using the CLI

To display the global IP routing statistics using the CLI, enter the following command from the prompt:

```
>#  show ip route summary
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

Refer to Table 6-26 for a definition of the I**P Routing Table Statistics** dialog box parameters:

***Table 6-26. IP Routing Table Statistics Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Current Number of Routes** | Displays the total number of active routes. |
| **Peak Number of Routes** | Displays the peak number of routes. |
| **Total Routes Added** | Displays the total number of routes added. |
| **Total Routes Deleted** | Displays the total number of routes deleted. |
| **RIP Route Changes** | Displays the number of changes to the IP route database made by RIP. |
| **RIP Queries** | Displays the number of RIP queries sent to the network. |

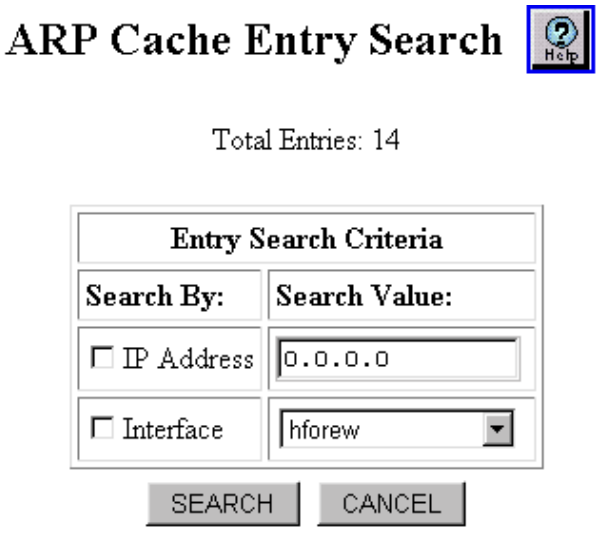
## Searching the IP ARP Cache

To search the IP ARP Cache entries:

1. Select **ARP Cache Search** from the **Routing > IP > Display** group on the Web Agent window. The **ARP Cache Entry Search** dialog box opens (Figure 6-49).

***Figure 6-49. ARP Cache Entry Search Dialog Box***

2. Select the search criteria you want to use to find more specific information on your switch's current ARP cache. For example, if you want to find all of the IP ARP cache entries associated with your out-of-band connection on your switch, search by **VLAN** and specify **Ethernet Console** as your search value.




3. Refer to Table 6-27 for an explanation of the **ARP Cache Search** dialog box parameters:

***Table 6-27. ARP Cache Search Dialog Box Parameters***

| Parameter | Allows you to do a search based on... |
|---|---|
| **IP Address** | The IP address you entered. |
| **Interface** | The interface you selected. System entries include all interfaces that you previously configured. |

4. Click SEARCH to start the search. If matching entries are found they are displayed in IP ARP Cache dialog box.

## IP Multicast Statistics

You can view IP Multicast statistics through by using either the Web Agent or the CLI. IP multicast statistics include:

- Displaying IGMP Global Statistics
- Displaying IGMP Interface Statistics
- Displaying the IGMP Local Multicast Forwarding Cache
- Displaying DVMRP Global Statistics
- Displaying DVMRP Interface Statistics
- Displaying DVMRP Neighbor Router(s)
- Displaying DVMRP Routing Table Statistics
- Displaying the DVMRP Route Table

- Displaying the DVMRP Upstream Routers
- Displaying the DVMRP Designated Forwarder(s) Table
- Displaying the DVMRP Downstream Dependent Router(s)
- Displaying the DVMRP Multicast Forwarding Cache

*** Note:** It is possible to use **access rules** to filter and prioritize multicast traffic.

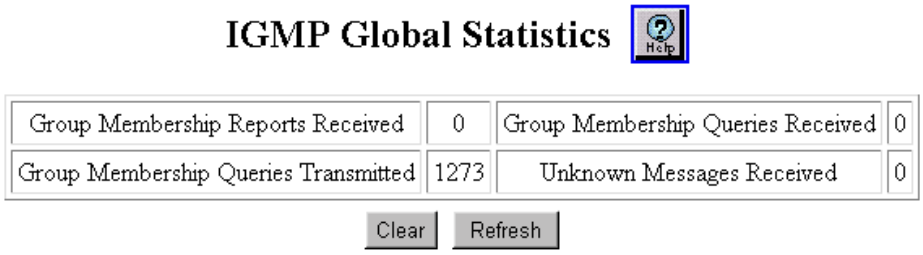
## Displaying IGMP Global Statistics Using the Web Agent

IGMP global statistics provides membership reports, membership queries transmitted and received, and unknown messages.

To display IGMP global statistics from the Web Agent:

1. Select **Global Statistics** from the **Routing > IGMP** group on the Web Agent window. The **IGMP Global Statistics** dialog box opens (Figure 9-26).

***Figure 6-50. IGMP Global Statistics Dialog Box***




2. To modify your global statistics, perform one of the following:
   - Click **CLEAR** to reset all statistics to zero
   - Click **REFRESH** to view the latest statistics.

3. Refer to Table 6-28 for an explanation of the **IGMP Global Statistics** dialog box parameters:

*Table 6-28. IGMP Global Statistics Dialog Box Parameters*

| Parameter | Defines the... |
|---|---|
| **Group Membership Reports Received** | Number of reports received in response to a group membership query. Hosts respond to a Query by generating Host Membership Reports reporting each host group to which they belong on the network interface from which the Query was received. |
| **Group Membership Queries Transmitted** | Number of query messages sent by all local IGMP interfaces. These messages are sent to discover which host groups have members on their attached local networks. Queries are addressed to the all-hosts group (address 224.0.0.1), and carry an IP time-to-live of 1. |
| **Group Membership Queries Received** | Number of query messages received by all local IGMP interfaces. |
| **Unknown Messages Received** | IGMP message of a type *other* than Group Membership Query, Group Membership Report, or Leave group. |

# Displaying IGMP Interface Statistics

You can examine IGMP interface statistics for each configured IP interface with multicast protocol enabled through the **IGMP Interface Statistics** window.

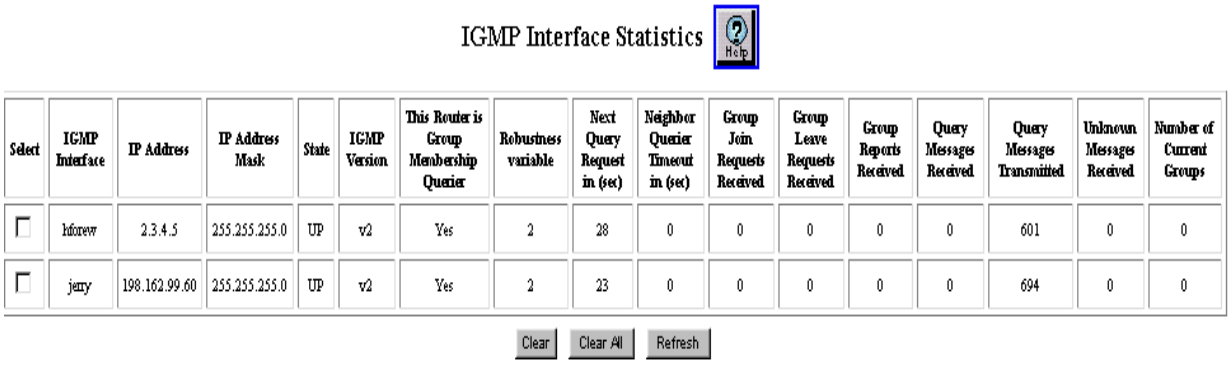
You can display IGMP interface statistics using either the Web Agent or the CLI.

## Displaying IGMP Interface Statistics Using the Web Agent

To display the IGMP Interface Statistics window using the Web Agent:

1. Select **Interface Statistics** from the **Routing > IGMP >** group on the Web Agent window. The **IGMP Interface Statistics** dialog box opens (Figure 9-27).

*Figure 6-51. IGMP Interface Statistics Dialog Box*




2. To modify the interface statistics, perform one of the following:

   — Select one or more interfaces, and then *c*lick **CLEAR** to reset statistics on those interfaces to zero.

   — Click **CLEAR ALL** to reset all statistics to zero.

   — *C*lick **REFRESH** to view the latest interface statistics.

3. Refer to Table 6-29 fro an explanation of the **IGMP Interface Statistics** dialog box parameters:

*Table 6-29. IGMP Interface Statistics Dialog Box Parameters*

| Parameter | Defines the... |
|---|---|
| **IGMP Interface** | IP interface for these statistics. |
| **IP Address** | IP address associated with the interface. |
| **IP Address Mask** | Subnet mask associated with each listed interface. |
| **State** | Current state of the interface. For example, if the interface is enabled and operating properly, UP is displayed. |
| **IGMP Version** | Version of IGMP enabled on each interface.The default version is V2 |
| **This Router is Group Membership Querier** | Router that was configured or elected to be the designated **group membership querier**. The switch queries hosts on each interface only when it is acting as the designated querier on that interface. |
| **Robustness Variable** | Setting for the expected packet loss on a subnet. If a subnet is expected to have more packet loss, the Robustness Variable should be increased. The Robustness Variable must not be set to 0 and should not be set to 1.<br>The default value is 2 |
| **Next Query Request (sec)** | Remaining amount of time (in seconds) before the next group membership query is transmitted. |

*Table 6-29. IGMP Interface Statistics Dialog Box Parameters continued*

| Parameter | Defines the... |
|---|---|
| **Neighbor Querier Timeout (sec)** | Amount of time (in seconds) remaining before this interface assumes the role of designated querier. This timer is reset to the value entered for the Neighbor Querier Timeout Interval each time an IGMP query is received from a neighbor with a lower IP address. If no response is received in the allowed time, the switch will become the designated querier on this interface. Applicable only if IGMP V2 is used. |
| **Group Join Requests Received** | Number of new groups on this interface. |
| **Group Leave Requests Received** | Number of leave requests received on this interface. |
| **Group Reports Received** | Number of reports received on this interface in response to a group membership query. Hosts respond to a Query by generating Host Membership Reports reporting each host group to which they belong on the network interface from which the Query was received. |
| **Query Messages Received** | Number of query messages received from other multicast routers. |
| **Query Messages Transmitted** | Number of query messages sent by a multicast router. These messages are sent to discover which host groups have members on their attached local networks. Queries are addressed to the all-hosts group (address 224.0.0.1), and carry an IP time-to-live of 1. |
| **Unknown Messages Received** | IGMP messages received with an unsupported type. |
| **Number of Current Groups** | Number of groups on each interface for which there are entries in the Group Membership Table. |

## Displaying IGMP Interface Statistics Using the CLI

To display the IGMP Interface Statistics window using the CLI, enter the following command from configuration mode:

```
(configure)# show ip igmp statistics
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

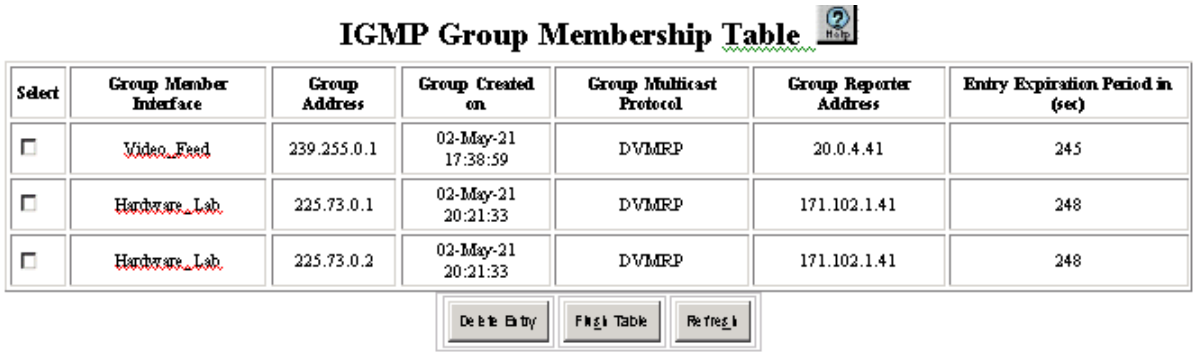
# Displaying the IGMP Group Membership Table

The multicast group table provides information on interfaces that are members of an IGMP group and contains an expiry time for the entry, IP address of the group, and the group reporter address.

To display the multicast group table using the Web Agent:

1. Select **Group Membership Table** from the **Routing > IGMP** group on the Web Agent window. The **IGMP Group Membership Table** dialog box opens.

*Figure 6-52. IGMP Group Membership Table Dialog Box*




2. To modify the **IGMP Group Membership Table**, perform one of the following steps:
   - Select the entry and click **Delete Entry** to delete one or more entries.
   - Click **Flush Table** to clear the entire table.
   - Click **REFRESH** to receive the most up-to-date information on the entries in the table.
3. Refer to Table 6-30 for an definition of the **IGMP Group Membership Table** dialog box parameters:

*Table 6-30. IGMP Group Membership Table Dialog Box Parameters*

| Parameter | Defines the... |
|---|---|
| **Group Member Interface** | Interface that is connected to a member of an IGMP group. |
| **Group Address** | Group address that has members on this interface. |

*Table 6-30. IGMP Group Membership Table Dialog Box Parameters continued*

| Parameter | Defines the... |
|---|---|
| **Group Created On** | Time at which the group was created on the router. |
| **Group Multicast Protocol** | Routing protocol being used for the group. If no routing protocol is being used on the interface a group is on, this column displays IGMP. |
| **Group Reporter Address** | IP address of the host that sent the most recent host membership report for this group. |
| **Entry Expiration Period in (sec)** | Expiration time (in seconds) of the group that is being displayed. |

### Display the Multicast group table from the CLI

To display the multicast group table using the CLI, enter the following command from configuration mode:

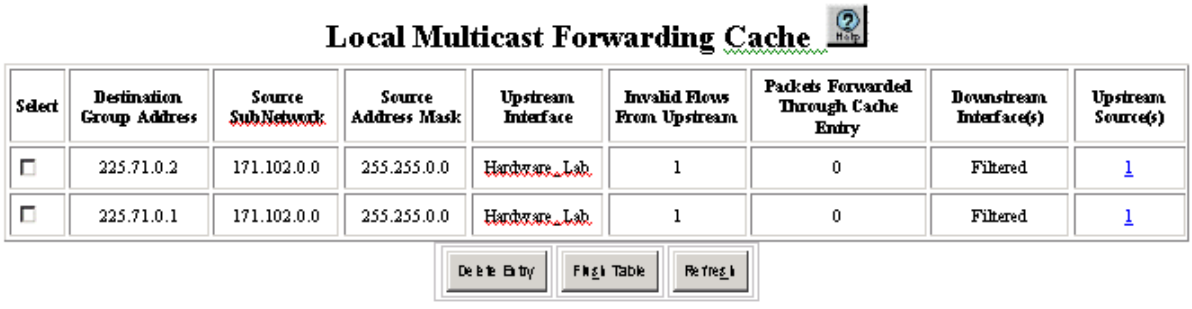
```
(configure)# show ip igmp groups
```

## Displaying the IGMP Local Multicast Forwarding Cache

To display the multicast forwarding cache information (IGMP only interfaces):

1. Select **Local Multicast Forwarding Cache** from the **Routing > IGMP** group on the Web Agent window. The **Local Multicast Forwarding Cache** dialog box opens.

*Figure 6-53. Local Multicast Forwarding Cache Dialog Box*




2. To modify the Local Multicast Forwarding Cache, select an entry and:

— Click **Delete Entry** to delete one or more entries.

— Click **Flush Table** to clear the entire table.

— Click **REFRESH** to receive the most up-to-date information on the entries in the table.

3. Refer to Table 6-31 to review the IGMP Multicast Forwarding Cache information:

*Table 6-31. IGMP Local Multicast Forwarding Cache Parameters*

| Parameters | Defines the... |
|---|---|
| **Destination Group Address** | Destination group address of the multicast transmission. |
| **Source SubNetwork** | Subnet on which the IGMP interface(s) exist. |
| **Source Address Mask** | Subnet mask associated with the IGMP source subnetwork. |
| **Upstream Interface** | IP interface configured on the upstream interface. |
| **Invalid Flows From Upstream** | Number of invalid flows received from the upstream neighbor. |
| **Packets Forwarded Through Cache Entry** | Number of packets successfully forwarded in the CPU (supervisor module). |
| **Downstream Interface(s)** | Number of downstream interfaces and provides a link to the IGMP Downstream Interfaces dialog box. |
| **Upstream Source(s)** | Number of upstream interfaces and provides a link to the IGMP Upstream Interfaces dialog box. |

# Displaying DVMRP Global Statistics

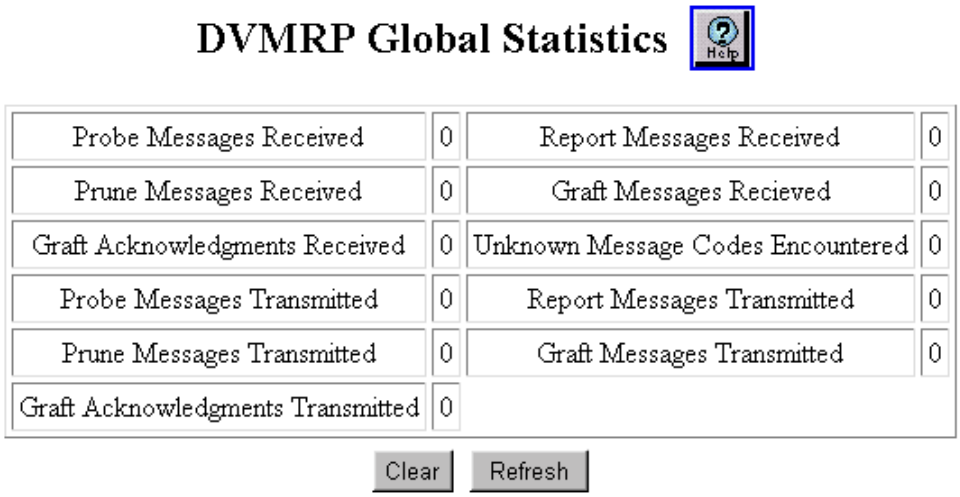
You can view the DVMRP Global Statistics from by using either the Web Agent or the CLI.

## Displaying DVMRP Global Statistics by Using the Web Agent

To display the DVMRP global statistics:

1. Select **Global Statistics** from the **Routing > DVMRP** group on the Web Agent window. The **DVMRP Global Statistics** dialog box opens (Figure 6-54).

*Figure 6-54. DVMRP Global Statistics Dialog Box*




2. Click:
   - **CLEAR** to reset all statistics to zero
   - **REFRESH** to view the latest statistics.
3. Refer to Table 6-32 for an explanation of the **DVMRP Global Statistics** dialog box parameters:

*Table 6-32. DVMRP Global Statistics Dialog Box Parameters*

| Statistic | Defines the number of... |
|---|---|
| **Probe Messages Received** | Probe messages received on this switch. DVMRP routers exchange probes and routing updates so they each have a picture of their neighbors' capabilities and the DVMRP network topology. |
| **Report Messages Received** | Route Report messages received on this switch. |
| **Prune Messages Received** | Prune messages received on this switch. This indicates the number of old branches removed from the multicast distribution tree. |
| **Graft Messages Received** | Graft messages received. This indicates the number of attempts at adding a new branch to the multicast distribution tree. |
| **Graft Acknowledgments Received** | Graft acknowledgments received. |
| **Unknown Message Codes Encountered** | Messages received that are not graft, report, or probe messages. |
| **Probe Messages Transmitted** | Probe messages transmitted to the network. |
| **Report Messages Transmitted** | Report messages transmitted on this switch. |

*Table 6-32. DVMRP Global Statistics Dialog Box Parameters continued*

| Statistic | Defines the number of... |
|---|---|
| **Prune Messages Transmitted** | Prune messages transmitted upstream on this switch. This indicates the number of old branches removed from the multicast distribution tree. |
| **Graft Messages Transmitted** | Graft messages transmitted upstream from this switch. This indicates the number of new upstream branches added to the multicast distribution tree. |
| **Graft Acknowledgments Transmitted** | Graft acknowledgments sent downstream from this switch. This indicates the number of new downstream branches added to the multicast distribution tree. |

# Displaying DVMRP Interface Statistics

DVMRP interface statistics list active DVMRP interfaces and provide specific information on each interface.

To display DVMRP interface statistics using the Web Agent:

1. Select **Interface Statistics** from the **Routing > DVMRP** group on the Web Agent window. The **DVMRP Interface Statistics** dialog box opens (Figure 6-55).

*Figure 6-55. DVMRP Interface Statistics Dialog Box*

**DVMRP Interface Statistics**

| Select | DVMRP Interface | Network Address | Address Mask | State | Type | Metric | IGMP Querier on Interface | Next Probe Message in (sec) | Unrecognized Packets Received | Invalid Routes Received | Neighbor DVMRP Router(s) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 13 | 10.0.1.129 | 255.255.255.128 | UP | Broadcast | 1 | Yes | 2 | 0 | 0 | 0 |
| ☐ | vlan_10.0.3.1_jwiebe | 10.0.3.1 | 255.255.255.128 | UP | Broadcast | 1 | Yes | 2 | 0 | 0 | 0 |
| ☐ | 18 | 10.0.4.1 | 255.255.255.128 | UP | Broadcast | 1 | Yes | 2 | 0 | 0 | 0 |
| ☐ | 22 | 10.0.6.1 | 255.255.255.128 | UP | Broadcast | 1 | Yes | 2 | 0 | 0 | 0 |
| ☐ | 23 | 10.0.6.129 | 255.255.255.128 | Down | Broadcast | 1 | No | 2 | 0 | 0 | 0 |
| ☐ | 50 | 192.168.50.100 | 255.255.255.0 | UP | Broadcast | 1 | Yes | 3 | 0 | 0 | 0 |
| ☐ | Inet_inband | 10.0.7.1 | 255.255.255.128 | Down | Broadcast | 1 | No | 3 | 0 | 0 | 0 |

Clear | Clear All | Refresh

2. Select an interface and perform one of the following:
   - Click **REFRESH** to view the latest interface statistics.
   - Click **CLEAR All** to reset all statistics to zero.
   - Click **CLEAR** to reset the selected interface.

3. Refer to Table 6-33 for an explanation of the **DVMRP Interface Statistics** dialog box parameters:

*Table 6-33. DVMRP Interface Statistics Parameters*

| Parameter | Defines the... |
|---|---|
| **DVMRP Interface** | IP interface configured with the DVMRP multicast routing protocol. |
| **Network Address** | IP address of the interface configured with the DVMRP multicast. |
| **Address Mask** | IP subnet mask associated with the interface. |
| **State** | Current status of the interface. Possible status indications include:<br>• **UP** - The interface is active.<br>• **DOWN** - The interface is inactive. |
| **Type** | Type of interface configured. Possible values include:<br>• **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation.<br>• **IPIP Tunnel** - All multicast traffic (data and protocol messages) on this interface is encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP).<br>• **Non-Encapsulated Tunnel** - All multicast data traffic on this interface is IPIP encapsulated, but the protocol messages are simple unicast. |
| **Metric** | Interface cost. |
| **IGMP Querier on Interface** | Router is the IGMP querier. The purpose of the IGMP querier is to periodically poll hosts on your network to trigger group membership reports. |
| **Next Probe Message in (sec)** | Time (in seconds) remaining until the next probe message is sent. |
| **Unrecognized Packets Received** | Number of unknown DVMRP messages. |
| **Invalid Routes Received** | Number of invalid routes received on this interface. |
| **Neighbor DVMRP Router(s)** | Number of (neighbor) routers that are also running DVMRP.<br>**Note:** This number is a hypertext link that provides additional information on the DVMRP neighbor router(s). |

### Displaying DVMRP Interface Statistics using the CLI

To display the DVMRP interface statistics using the CLI, enter the following command from configuration mode:

```
(configure)# show ip dvmrp interface
```

## Displaying DVMRP Neighbor Router(s)

To view the DVMRP neighbor routers using the Web Agent:

1. Select Interface Statistics from the **Routing > DVMRP** group on the Web Agent window. The **DVMRP Interface Statistics** dialog box opens (Figure 6-55).

*Figure 6-56. DVMRP Neighbor Routes Dialog Box*

2. Select the number in the **Neighbor DVMRP Router(s)** column, if it is 1 or more. The **DVMRP neighbor routers** dialog box opens.
3. Refer to Table 6-34 to view more information on DVMRP neighbor routers.

*Table 6-34. DVMRP Neighbor Routers*

| Parameter | Displays... |
|---|---|
| **Neighbor Network Address** | The neighbor router's IP address. |
| **Found on Interface** | The neighbor routers found on this interface. |
| **DVMRP Supported Major/Minor Version** | The DVMRP version supported by the neighbor router. |
| **Expiration period in (sec)** | The time (in seconds) before the neighbor router times out. |

*Table 6-34. DVMRP Neighbor Routers continued*

| Parameter | Displays... |
|---|---|
| **Neighbor Received Probe From This Router** | Whether the neighbor router received this router's probe message. |
| **Neighbor Supports Prune Function** | Whether the neighbor router supports prune functionality. |
| **Neighbor Supports Generation ID Function** | Whether the neighbor router supports generation of IDs. |
| **Neighbor Supports MTRACE Requests** | Whether the neighbor router supports MTRACE requests. |
| **Neighbor is SNMP Manageable** | Whether the neighbor router can be managed by SNMP. |

### Displaying DVMRP Neighbor routers using the CLI

To display the DVMRP neighbor routers using the CLI, enter the following command from configuration mode:

```
(configure)# show ip dvmrp interface neighbors
```

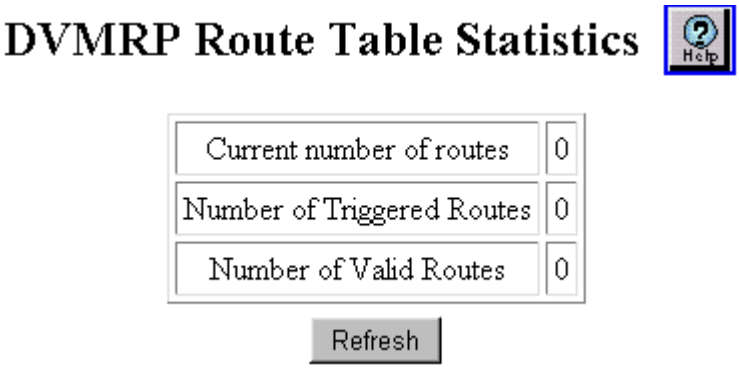
## Displaying DVMRP Routing Table Statistics

DVMRP routing table statistics provides information on the current number of valid routes, the number of total routes present (both valid and invalid), and the number of triggered routes.

To view the DVMRP routing table statistics using the Web Agent:

1. Select **Route Table Statistics** from the **Routing > DVMRP** group on the Web Agent window. The **DVMRP Routing Table Statistics** dialog box opens (Figure 6-57).

*Figure 6-57. DVMRP Route Table Statistics Dialog Box*




2. Refer to Table 6-35 for an explanation of the **DVMRP Route Table Statistics** dialog box parameters:

***Table 6-35. DVMRP Routing Statistical Parameters***

| Parameter | Defines the... |
|---|---|
| **Current Number of Routes** | Total number of routes present in the routing database. This number includes both valid and invalid routes. |
| **Number of Triggered Routes** | Total number of routes added to the routing table that were triggered by a topology change in the network. |
| **Number of Valid Routes** | Total number of *valid routes* present in the routing database. |

## Displaying the DVMRP Route Table

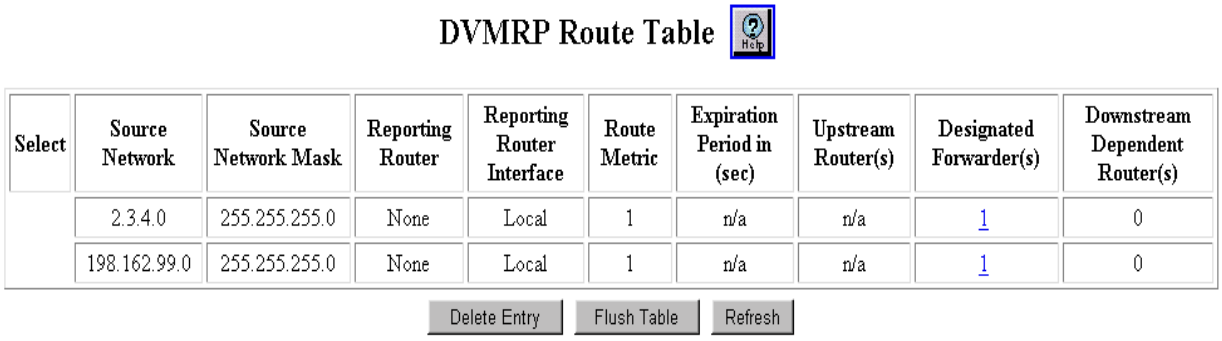
The DVMRP route table contains information on valid DVMRP routes, the expiry for those routes, and additional next-hop information.

To view the DVMRP route table using the Web Agent:

1. Select **Route Table** from the **Routing > DVMRP** group on the Web Agent window. The **DVMRP Route Table** dialog box opens (Figure 6-58).

***Figure 6-58. DVMRP Route Table Dialog Box***

2. To modify your DVMRP Route table, do one of the following:
   - To delete one or more entries., select the entry and click **Delete Entry**
   - To clear the entire table, click **Flush Table**.
   - To receive the most up-to-date information on the entries in the table, Click **REFRESH**.




3. Refer to Table 6-36for an explanation of the **DVMRP Route Table** parameters:

***Table 6-36. DVMRP Route Table Parameters***

| Parameter | Defines the... |
|---|---|
| **Source Network** | Network from which a multicast flow may originate. |
| **Source Network Mask** | Source network mask. |
| **Reporting Router** | IP address of the router reporting this route to its neighbors. |
| **Reporting Router Interface** | IP interface configured, which leads to the upstream neighbor (DVMRP router). |
| **Route Metric** | Router's cost to source network. |
| **Expiration Period in (sec)** | Time (in seconds) remaining before the source network is removed from the DVMRP routing table. |
| **Upstream Router(s)** | IP address of the DVMRP router that is the upstream neighbor to the local router. The local DVMRP router must know which DVMRP router is its upstream neighbor to determine how packets from a given source will be transmitted to a given multicast group. Opens DVMRP Upstream Router(s) dialog box. |
| **Designated Forwarder(s)** | Network router(s) responsible for forwarding from the source network onto the downstream interface. Opens the Designated Forwarders dialog box. |
| **Downstream Dependent Router(s)** | Number of downstream DVMRP routers that are dependent on this router for this particular route. Opens the DVMRP Downstream Dependent Router(s) dialog box. |

## Displaying the DVMRP Routing Table, using the CLI

To display the DVMRP route table using the CLI, enter the following command from configuration mode:

```
(configure)# show ip dvmrp routes
```

## Displaying the DVMRP Upstream Routers

To view the DVMRP upstream routers:

1. Select **Route Table** from the **Routing > DVMRP** group on the Web Agent window, The **DVMRP Route Table** dialog box opens (Figure 6-58).
2. Select the number in the **Upstream Router(s)** column to view information on the upstream routers. The U**pstream Router(s)** dialog box opens.
3. Refer to Table 6-37 for an explanation of the DVMRP Upstream Router(s) dialog box parameters.

***Table 6-37. DVMRP Upstream Router(s) Dialog Box Parameters***

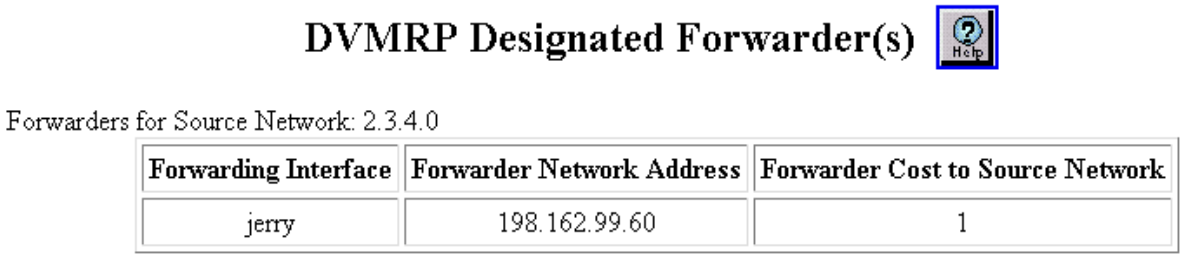
| Parameter | Definition |
|---|---|
| **Router Network Address** | Displays the router network address. |
| **Router Cost to Source Network** | Displays the cost metric. |
| **Found on Interface** | Displays the interface on which the upstream router was found. |

## Displaying the DVMRP Designated Forwarder(s) Table

To view the DVMRP Designated Forwarder table:

1. Select **Route Table** from the **Routing > DVMRP** group on the Web Agent window. The **DVMRP Route Table** dialog box opens (see Figure 6-58).
2. Select the number from the **Designated Forwarder** column for the appropriate source network. The **Designated Forwarder(s) Table** dialog box opens (see Figure 6-59).

***Figure 6-59. Designated Forwarder(s) Table Dialog Box***




3. Refer to Table 6-38 for an explanation of the **DVMRP Designated Forwarder(s)** dialog box parameters:

***Table 6-38. DVMRP Designated Forwarder(s) Table Dialog Box Parameters***

| Parameter | Defines the... |
|---|---|
| **Forwarding Interface** | Local interface which leads to the network where the Designated Forwarder resides. |
| **Forwarder Network Address** | Designated Forwarder for the given source network on the indicated Forwarding Interface. |
| **Forwarder Cost to Source Network** | Cost reported by the Designated Forwarder for the given source network. |

## Displaying the DVMRP Downstream Dependent Router(s)

To view the DVMRP downstream dependent routers:

1. Select **Route Table** from the **Routing > DVMRP** group on the Web Agent window. The **DVMRP Route Table** dialog box opens (see Figure 6-58).
2. Select the number from the **Downstream Dependent Router(s)** column for the appropriate source network. The **Downstream Dependent Router(s)** dialog box opens.
3. Refer to Table 6-39 for an explanation of the **DVMRP Downstream Dependent Router(s)** dialog box parameters.s

***Table 6-39. DVMRP Downstream Dependent Router(s) Dialog Box Parameter***

| Parameter | Definition |
|---|---|
| **Router Network Address** | Displays the router network address of the downstream dependent router. |
| **Found on Interface** | Displays the name of the interface on which the downstream router was found. |

*Table 6-39. DVMRP Downstream Dependent Router(s) Dialog Box Parameter*

| Parameter | Definition |
|---|---|
| **DVMRP Supported Major/Minor Version** | Displays the DVMRP version supported. |
| **Router Received Probe from This Router** | Displays whether the router received a probe from this router. |
| **Router Supports Prune Function** | Displays whether this router supports prune functionality. |
| **Router Supports Generation ID Function** | Displays whether the router supports generation ID function. |
| **Router is SNMP Manageable** | Displays whether the router can be managed by SNMP. |

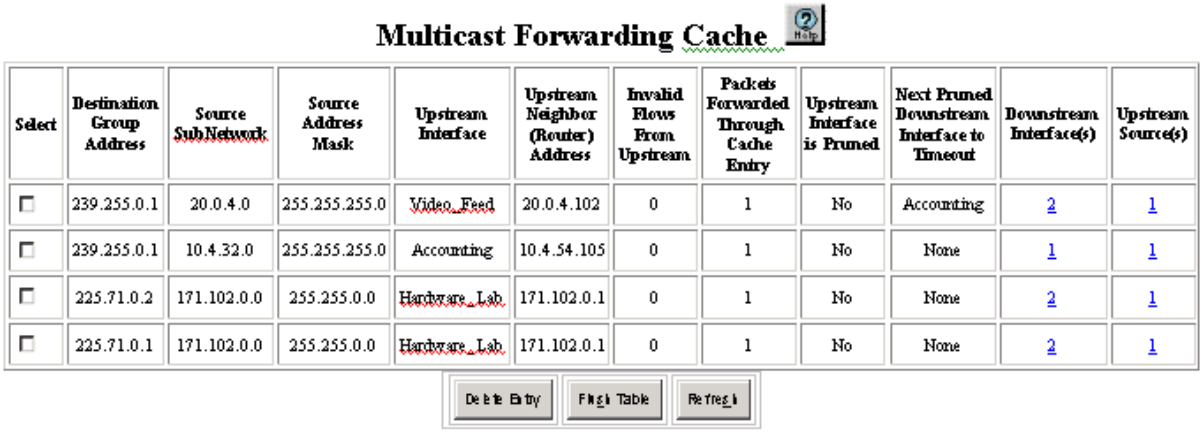
# Displaying the DVMRP Multicast Forwarding Cache

The DVMRP Multicast Forwarding Cache screen provides detailed information on the multicast forwarding attributes including information on downstream interfaces and upstream sources. DVMRP allows the switch to construct paths from the hosts that are sending to a multicast group to the hosts that are receiving it.

To display the multicast forwarding cache screen:

1. Select **Multicast Forwarding Cache** from the **Routing > DVMRP** group on the Web Agent window. The **Multicast Forwarding Cache** dialog box opens.(Figure 9-36)

*Figure 6-60. Multicast Forwarding Cache Dialog Box*


Multicast Forwarding Cache
Select
Destination Group Address
Source SubNetwork
Source Address Mask
Upstream Interface
Upstream Neighbor (Router) Address
Invalid Flows From Upstream
Packets Forwarded Through Cache Entry
Upstream Interface is Pruned
Next Pruned Downstream Interface to Timeout
Downstream Interface(s)
Upstream Source(s)
239.255.0.1 20.0.4.0 255.255.255.0 Video_Feed 20.0.4.102 0 1 No Accounting 2 1
239.255.0.1 10.4.32.0 255.255.255.0 Accounting 10.4.54.105 0 1 No None 1 1
225.71.0.2 171.102.0.0 255.255.0.0 Hardware_Lab 171.102.0.1 0 1 No None 2 1
225.71.0.1 171.102.0.0 255.255.0.0 Hardware_Lab 171.102.0.1 0 1 No None 2 1
Delete Entry
Flush Table
Refresh

2. To modify the Multicast Forwarding Table:
   - Select the entry and click **Delete Entry** to delete one or more entries.
   - Click **Flush Table** to clear the entire table.
   - Click **REFRESH** to receive the most up-to-date information on the entries in the table.
3. Refer to Table 6-40 for an explanation of the M**ulticast Forwarding Cache** dialog box parameters:

*Table 6-40. Multicast Forwarding Cache Dialog Box Parameters*

| Parameter | Defines the... |
|---|---|
| **Select** | Selection of the multicast forwarding cache. |
| **Destination Group Address** | Destination group address of the multicast transmission. |
| **Source SubNetwork** | Subnet from which the flow is coming. |
| **Source Address Mask** | Subnet mask associated with the DVMRP source subnetwork. |
| **Upstream Interface** | Local interface which is receiving this flow. |
| **Upstream Neighbor (Router) Address** | IP address of the upstream neighbor (router). |
| **Invalid Flows From Upstream** | Number of invalid flows received from the upstream neighbor. |
| **Packets Forwarded Through Cache Entry** | Number of packets successfully forwarded in the CPU (supervisor module) for this flow. |

*Table 6-40. Multicast Forwarding Cache Dialog Box Parameters continued*

| Parameter | Defines the... |
|---|---|
| **Upstream Interface is Pruned** | Router that is sending prunes to the upstream neighbor. Allows you to open the DVMRP Upstream Prune Information dialog box. |
| **Next Pruned Downstream Interface to Timeout** | Next interface that is currently pruned which will be grafted back. |
| **Downstream Interface(s)** | Number of downstream interfaces. Allows you to open the DVMRP Downstream Links dialog box. |
| **Upstream Source(s)** | Number of upstream interfaces. Allows you to open the Upstream Sources dialog box. |

4. Select the number in the **Upstream Interface is Pruned** field. The **Upstream Prune Information** dialog box opens.

5. Refer to Table 6-41 for an explanation of the Upstream Prune Information dialog box parameters.s

*Table 6-41. Upstream Prune Information Dialog Box Parameter*

| Parameter | Displays the... |
|---|---|
| **Destination Group Address** | Destination group address of the multicast session. |
| **Source SubNetwork** | Subnet on which the DVMRP interface exists. |
| **DVMRP Upstream Interface** | Name of the upstream interface. |
| **Interface Type** | The interface type. Types include:<br>• **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation.<br>• **IPIP Tunnel** - All multicast traffic (data and protocol messages) on this interface is encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP).<br>• **Non-Encapsulated Tunnel** - All multicast data traffic on this interface is IPIP encapsulated, but the protocol messages are simple unicast. |
| **Interface is Pruned** | Status of whether the interface has been pruned. |
| **Prune Expiration Time in sec** | Time (in seconds) that the interface times out waiting for the prune message to expire. |

6. Select the number in the **Downstream Interface(s)** field. The **DVMRP Downstream Link(s)** dialog box opens.

7. Refer to Table 6-42 for an explanation of the **DVMRP Downstream Links** dialog box parameters.

*Table 6-42. DVMRP Downstream Links Dialog Box Parameters*

| Parameter | Displays the... |
|---|---|
| **Destination Group Address** | Destination group address. |
| **Source SubNetwork** | Source subnetwork. |
| **DVMRP Downstream Interface** | DVMRP Downstream interface. |
| **Interface Type** | Interface type. Types include:<br>• **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation.<br>• **IPIP Tunnel** - All multicast traffic (data and protocol messages) on this interface is encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP).<br>• **Non-Encapsulated Tunnel** - All multicast data traffic on this interface is IPIP encapsulated, but the protocol messages are simple unicast. |
| **Interface is Pruned** | Status of whether the interface has been pruned. |
| **Prune Expiration in (sec)** | Time (in seconds) that the interface times out waiting for the prune message to expire. |

8. Select the number in the **Upstream Source(s)** field. The **DVMRP Upstream Source(s)** dialog box opens.

9. Refer to Table 6-43 for an explanation of the **DVMRP Upstream Source(s)** dialog box parameters..

*Table 6-43. DVMRP Upstream Source(s) Dialog Box Parameters*

| Parameter | Displays the... |
|---|---|
| **Destination Group Address** | Destination group address for the upstream interface. |
| **Flow Source Address** | Host source address for the upstream flow. |
| **Flow Upstream Interface** | Name of the flow source interface. |
| **Payload Protocol Type** | Protocol type for the payload. |
| **Source Port Number** | Source port number. |
| **Destination Port Number** | Destination port number. |

# Configuring Virtual Router Redundancy Protocol (VRRP)

VRRP is used to provide fast-fail over for hosts if the default gateway fails. This eliminates the single point of failure inherent in a network with statically configured default routes. The VRRP protocol defines an election process that will determine a Master and a Backup router. The Master router will forward all packets destined for the IP Address associated with the virtual router. The Backup router monitors the availability of the Master router and will assume Mastership in the event that the Master router fails.

The VRRP protocol is described in detail in RFC 2338.

## Globally Enabling VRRP

VRRP can be enabled (or disabled) globally using the Web or CLI. Disabling VRRP globally will cause all virtual routers to transition to the Initialize state (see State in table 8-3). VRRP is globally enabled by default.

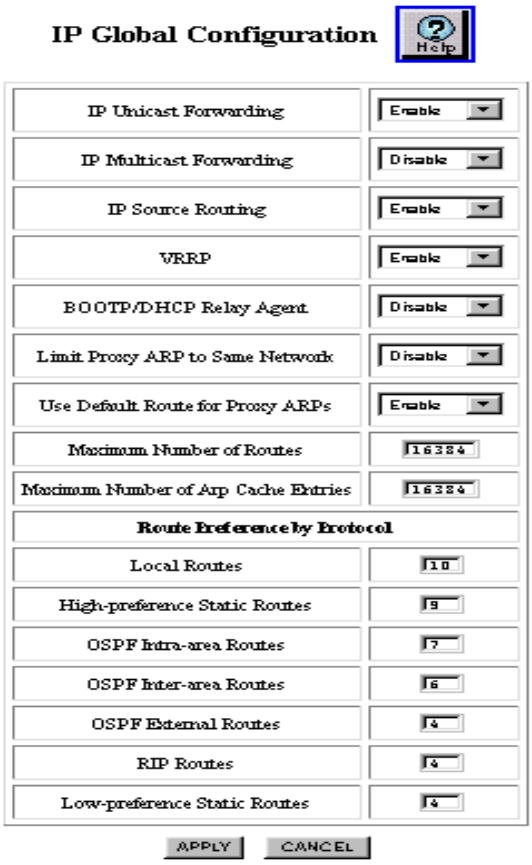
You can globally enable VRRP from either the Web Agent or the CLI.

### Web Agent Procedure

To globally enable VRRP using the Web Agent:

1. Select **Global Configuration** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Global Configuration** dialog box opens (Figure 6-61).

*Figure 6-61. IP Global Configuration Dialog Box*




2. Select **Enable** from the **VRRP** field pull-down menu.
3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### CLI Commands

To globally enable VRRP from the CLI, enter the following command in Configure mode:

```
<configure># router vrrp
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

## Enabling VRRP on an Interface

VRRP can be enabled on an interface using the Web Agent or the CLI.

*** Note:** For VRRP to function correctly, it must be enabled globally and enabled on the interfaces on which any virtual routers are to be created. Otherwise, any virtual routers created will be in the Initialize state (see State in table 8-3).

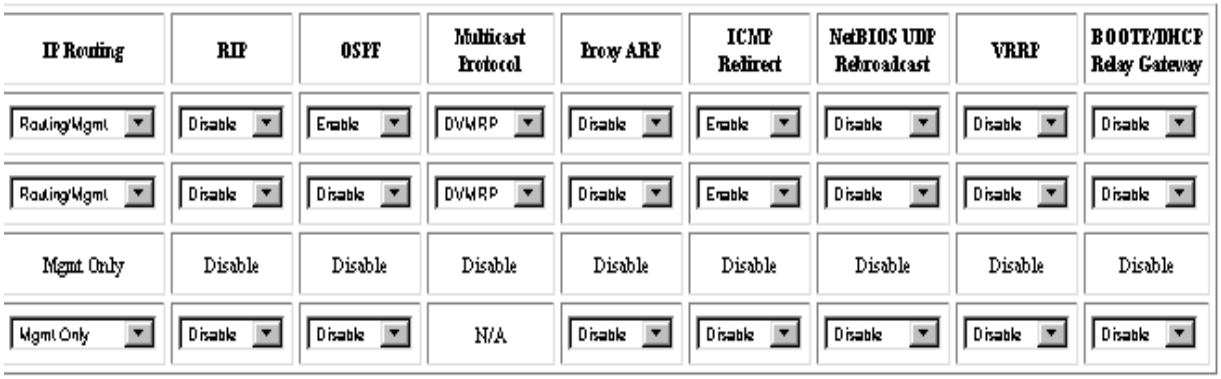
## Using the Web Agent

To enable an VRRP on an interface using the Web Agent:

1. Select **Interfaces** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Interfaces** dialog box opens (Figure 6-62).

   *** Note:** Due to the length of the IP Interfaces dialog box, it is divided into two figures in Figure 6-62.

***Figure 6-62. IP Interface Dialog Box***




2. Select the interface on which you want VRRP to be enabled.
3. Select **Enable** from the **VRRP** field pull-down menu for the interface you selected.
4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## CLI Command

To enable an VRRP on an interface using the CLI, enter the following command in Configure/Interface mode:

```
<config-if:<if name>>># ip vrrp
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Creating a VRRP Virtual Router

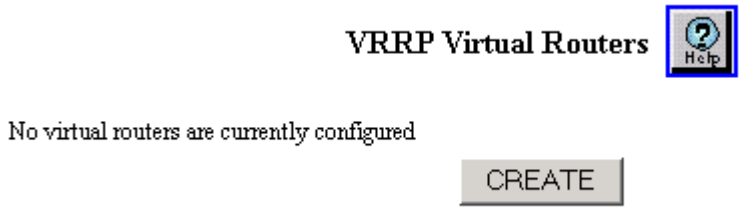
You can create a VRRP router using either the Web Agent or the CLI.

## Using the Web Agent

To create a VRRP router from the Web Agent:

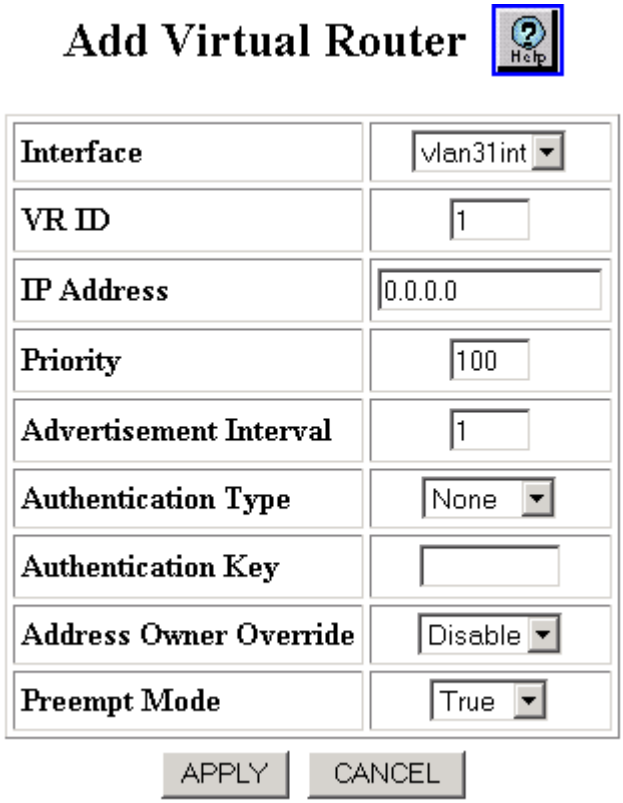
1. Select **VRRP** from the **Routing > IP > Configuration** group on the Web Agent window. The **VRRP Virtual Routers** dialog box opens (Figure 6-63).

*Figure 6-63. VRRP Virtual Routers Dialog Box*




2. Select **CREATE**. The **Add VRRP Virtual Router** dialog box opens (Figure 6-64).

*Figure 6-64. Add VRRP Virtual Router Dialog Box*



3. Table 6-44 lists the parameters and describes the type of information that should be entered in the **Add VRRP Virtual Router** dialog box fields to create a VRRP virtual router.

***Table 6-44. Add VRRP Virtual Router Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Interface** | This is the IP Interface that the virtual router will be associated with. The drop-down menu displays all the IP Interfaces currently created. Select the Interface that the virtual router will be associated with. Be sure to enable VRRP on the particular Interface selected. Multiple virtual routers may be created on a single interface but they must have unique IP Addresses and VRID's.<br><br>The default setting is the top interface in the Routing>IP>Configuration>Interface screen. |
| **VR ID** | This is the virtual router identification number. The range is 1 - 255. The same VR ID can be used for multiple virtual routers as long as the associated IP Interfaces are on different VLAN's (each VR ID number can be used once per VLAN).<br><br>The default value is 1.<br>The range is 1-255 (decimal). |
| **IP Address** | Enter the IP Address for the virtual router. This is known as the Virtual IP Address (VIP). The VIP can be the same as the IP Address of the associated Interface. This is known as IP Address Owner. The VIP can also be a unique address. This is called non-Address Owner. IP Address Owner and non-Address Owner are discussed in more detail below under VRRP Considerations. The VIP must be on the same subnet as the corresponding IP Interface.<br><br>The default value is 0.0.0.0. |
| **Priority** | Enter the Priority of the virtual router. If the router is the IP Address Owner of the VIP (as described above), then the Priority will automatically be set to 255 regardless of the value entered. If the router is not the owner of the VIP, than any value in the range of 1 - 254 can be entered. Note that the higher the value, the higher Priority the virtual router will have.<br><br>The default value is 100. |

*Table 6-44. Add VRRP Virtual Router Dialog Box Parameters continued*

| Parameter | Definition |
|---|---|
| **Advertisement Timer** | Enter the value of the Advertisement Interval in seconds. This is the time interval that the router will send out advertisements if it is the Master. The range is from 1 - 255 seconds. The Advertisement Interval also defines the time that a Backup will wait until becoming Master. A Backup will become Master if it does not receive an advertisement in approximately three times the Advertisement Interval value. An Advertisement Interval will allow for the fastest fail over time (approximately three seconds).<br><br>The default value is 1. |
| **Authorization Type** | Select the Authentication Type for this virtual router. If None is selected, then no Authentication Key will be used. If Simple is selected, then the virtual router will employ Simple Text Password authentication and use the password in the Authentication Key field (described below).<br><br>The default value is None. |
| **Authorization Key** | Enter the Authentication Key in this field. If the Authentication Type was set to None, then a password will not be used in the VRRP election process regardless if one is entered in this field. If the Authentication Type was set to Simple, then the password entered here will be used to verify correct configuration of the corresponding virtual routers involved in the VRRP election process. The password must be an alphanumeric string from 0 - 8 characters and is case-sensitive. Leaving this field blank is also a valid password.<br><br>If a blank field password is desired, set the Authentication Type to None and leave the Authentication field blank. After the virtual router is created, select and modify it and set the Authentication Type to simple.<br><br>A password may also be entered without selecting Simple in the Authentication Type field. In this case, the password will be stored but not used until the Authentication Type is set to Simple.<br><br>This field is blank by default. |

*Table 6-44. Add VRRP Virtual Router Dialog Box Parameters continued*

| Parameter | Definition |
|---|---|
| **Address Owner Override** | Enable or Disable Address Owner Override using the drop-down menu. Enabling Address Owner Override allows the VIP to reply to ICMP requests if the router is not the IP Address owner of the virtual router's IP Address (the VIP and IP Address are different). Address Owner Override helps to ensure connectivity and availability of all virtual routers.<br><br>*** Note:** This parameter is not defined in the VRRP RFC 2338.<br><br>The default value is Disable |
| **Preempt Mode** | Enable or disable Preempt Mode using the drop-down menu. Preempt Mode will allow a Backup virtual router with a higher Priority to preempt a Master virtual router with a lower Priority. Note that the router that owns the IP Address associated with the virtual router will always preempt regardless if this is enabled or disabled. To disable this feature, set this field to False.<br><br>The default value is True. |

4. Click **CREATE** to save your changes, or **CANCEL to restore previous settings.**

### Using the CLI

To create a VRRP router from the CLI, enter the following command in Configure mode:

```
<config-if:<interface name>># ip vrrp <vr-id>(1-255) address (ip-address)
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

## Displaying VRRP Statistics

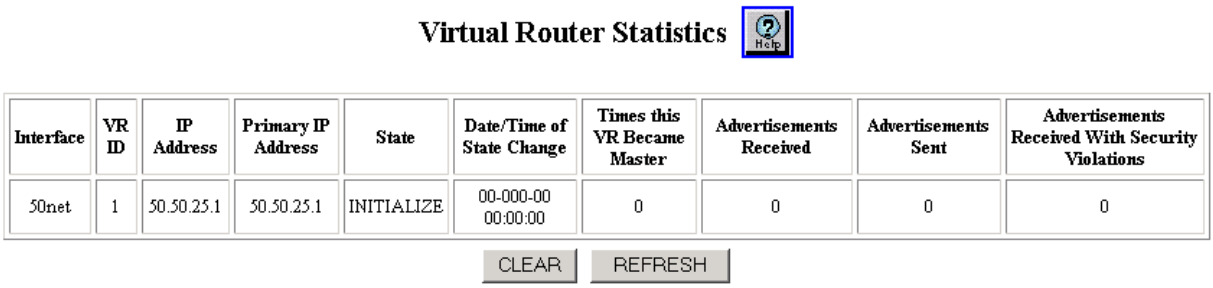
You can display VRRP router statistics by using either the Web Agent or the CLI.

### Using the Web Agent

To display VRRP virtual router statistics using the Web Agent:

1. Select **VRRP Statistics** from the **Routing > IP > Display** group on the Web Agent window. The **VRRP Virtual Router Statistics** dialog box opens (Figure 6-65).

*Figure 6-65. VRRP Virtual Router Statistics Dialog Box*




2. To modify the VRRP statistics:
   - Click **CLEAR** to reset all the entries.
   - Click **REFRESH** to receive the most up-to-date information on the entries.
3. Refer to Table 6-45 for an explanation of the **VRRP Virtual Router Statistics** dialog box parameters:

*Table 6-45. VRRP Virtual Router Statistics Dialog Box Parameters*

| Parameter | Definition... |
|---|---|
| **Interface** | Displays the IP Interface name that the virtual router is associated with. |
| **VR ID** | Displays the virtual router identification number. |
| **IP Address** | Displays the IP Address of the virtual router. It is also known as the virtual IP Address (VIP). |
| **Primary IP Address** | The Primary IP address is the real IP address of the IP interface that a virtual router is associated with.This address can be viewed in the VRRP statistics page of the web agent.<br>**Note:** For more information about the Primary IP Address see the section titled *"Changing the Primary IP Address"*. |

*Table 6-45. VRRP Virtual Router Statistics Dialog Box Parameters continued*

| Parameter | Definition... |
|---|---|
| **State** | Displays the current state of the virtual router.<br>·**Initialize** - Indicates that the virtual router is waiting for a Startup Event. A virtual router could be in this state due to VRRP being disabled Globally, VRRP being disabled on the corresponding IP Interface, or that the associated IP Interface is Down.<br>·**Backup** - Indicates that the virtual router is in the Backup state. A virtual router in this state monitors the availability of the Master router.<br>·**Master** - Indicates that the virtual router is in the Master state. A virtual router in this state functions as the forwarding router for the associated IP Address |
| **Date/Time of State Change** | Displays the date and time when the last state change occurred. This value is displayed in year-month-day and hh:mm:ss. |
| **Times this VR Became Master** | Displays the number of times this virtual router became the Master router. |
| **Advertisements Received** | Displays the number of advertisements received by this virtual router. |
| **Advertisements Sent** | Displays the number of advertisements sent by this virtual router. |
| **Advertisements Received with Security Violations** | Displays the number of advertisements that were discarded by this virtual router. An advertisement is discarded if it contains incorrect parameters. |

## Using the CLI

To view VRRP virtual router statistics using the CLI, enter the following command in User mode:

```
> show ip vrrp [cr|<if-name>|<detail>]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# VRRP Configuration Considerations

## Selecting VR ID numbers for Virtual Routers

The allowable range for the VR ID of a virtual router is 1-255. For easiest troubleshooting and identification, it is recommended that each virtual router have a unique VR ID. Duplicate VR ID's are allowed, however, as long the IP Interfaces they are associated with are on different VLAN's. Because of this, VRRP cannot be configured in a multinetted network.

## Assigning the IP Address of a Virtual Router

When creating a virtual router, it must be first decided whether to make the IP Address of the virtual router (the VIP) unique or the same as the Primary IP Address of the associated IP Interface address. If the VIP is unique, this is known as non-IP Address Owner. This means the VIP is not "owned" by the router as a Primary IP Address. If the VIP is not unique, meaning it matches the Primary IP Address of the associated IP Interface, then this is known as IP Address Owner. The VIP Address is "owned" by the associated IP Interface. Each method will be discussed below in more detail.

## IP Address Owner Features

IP address owner allows for the highest possible priority. A Priority of 255 is reserved for IP Address Owner. In a properly configured network, there will never be a virtual router with a higher priority (if there is another virtual router on the same subnet with a priority of 255, then the network is misconfigured with duplicate IP Addresses). This means that this virtual router will always assume Mastership if it is available to do so.

IP address owner features are:

- Requires less configuration. The Priorities are automatically assigned. Backup routers can use the default Priority settings and correct Master-Backup election will be achieved.
- Another IP Address does not have to be reserved for the virtual router. This is helpful if IP Addresses are scarce or limited.
- Preempt mode cannot be disabled. A virtual router that is IP Address Owner will always preempt and assume Mastership from a Backup router.
- A virtual router that is IP Address Owner will "overwrite" the MAC Address of the associated IP Address. In the ARP Cache Table, the MAC Address of the IP Address will be the VRRP MAC.

## Non-Address Owner Features

Non-address owner features are:

- Requires more configuration but allows for more control and customization of the Priorities of each virtual router.
- The virtual router IP Address and associated IP Address will both be displayed in the ARP Cache Table. This is helpful for troubleshooting and identification.
- Preempt Mode can be used. As described in the "IP Address Owner Features" section, if the Preempt Mode is set to False, then a higher Priority virtual router will not assume Mastership from a virtual router that is currently Master. This is helpful when a router goes down and the Backup router becomes Master. When the original router comes back online, it will not take Mastership from the current Master. This will allow the current traffic to remain unchanged. Another state change will only occur if the current Master router goes down. This is especially helpful in a network where a routing protocol is used (RIP, OSPF). In most cases, the VRRP election process will take place before the routing table has been updated. This may cause a longer period of traffic loss.

## Assigning Priorities to Virtual Routers

The allowed configurable range for the Priority of a virtual router is 1-254. 255 is reserved for a virtual router that is IP Address Owner (as described above). If two routers are participating in VRRP, making the desired Master router 254 (or 255 if IP Address Owner) and the Backup router 100 (the default Priority) is a common configuration. If multiple routers will be backing up the Master router, then the Priorities can be assigned in descending order (100, 99, 98, etc., for example).

Equal Priorities are also allowed but may be more difficult to troubleshoot. If two Master routers have the same Priority (and the same VRRP settings), the VRRP election process then checks the associated IP Address of each virtual router. In that case, the associated IP Address with a higher value becomes Master. However, if a Master and Backup virtual router have the same Priority, the Backup will not become Master even if it has a higher associated IP Address. In other words, equal priorities are not enough for a backup router that is already in the Primary state to become Backup.

## Selecting an Advertisement Interval

In most cases, leaving the Advertisement Interval to its default value of 1 is adequate. Usually, this is also desired because it will allow for the fastest fail over time. As described above, the time a Backup will become Master if it stops receiving advertisements is approximately three times this value in seconds. A higher value may be selected if the network is very stable and less advertisement traffic is desired. In any case, it is not recommended that the interval be increased to values above five or six.

## Deciding to Use Authentication

In networks where there is little or no security risk and a minimal chance of miscommunication, authentication is probably not needed. Using Simple Text Password authentication can provide protection against accidental misconfiguration. The correct password must be entered for a new virtual router before it will begin the VRRP election process with another virtual router. Simple Text Password authentication does not provide protection from hostile attacks.

## Changing the Primary IP address

If there is a virtual router that is an IP Address Owner created on an IP interface, the priority will be changed to 100 (default) if the Primary IP Address is changed, because a Priority of 255 is reserved for the IP Address Owner only.

If the virtual router is a non-Address Owner and the associated Primary IP Address is changed to the same as the virtual router IP Address, the Priority of that virtual router is changed to 255, since it is now the IP Address Owner.

If the Primary IP Address is changed so that it is no longer on the same subnet as an associated virtual router, the virtual router will be deleted

# Configuring ICMP Router Discovery Protocol (IRDP)

IRDP is an alternative router discovery protocol using ICMP messages on multicast links. ICMP uses router discovery messages, known as router advertisements and router solicitations.

Each router periodically multicasts a router advertisement from each of its multicast interfaces, announcing the IP address of that interface, and other router IP addresses. Hosts discover the addresses of their neighbor routers by listening for the advertisements. When a host attached to a link starts up, it may multicast a router solicitation to ask for immediate advertisements, rather than waiting for the next periodic one to arrive.

If no advertisements arrive, the host re-transmits the solicitation, but does not send additional solicitations. Routers that subsequently start up, or were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

## Enabling IRDP on an Interface

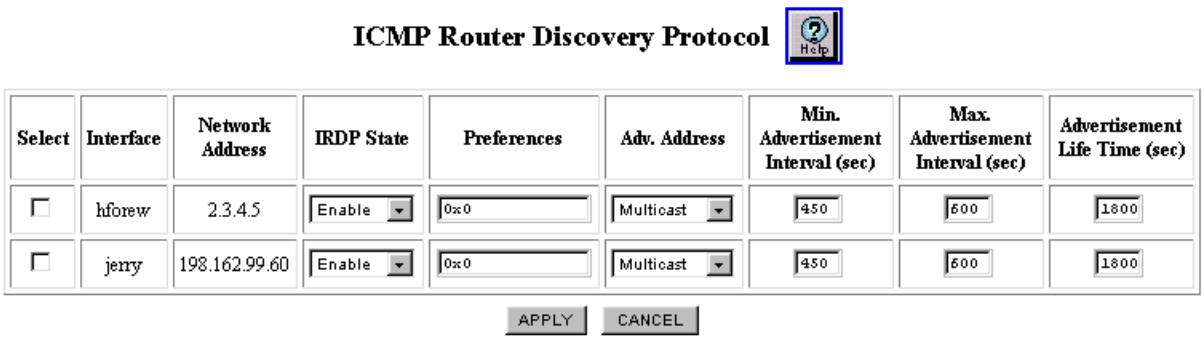
You can enable IRDP on an interface using either the Web Agent or the CLI.

### Using the Web Agent

To enable IRDP on an interface using the Web Agent:

1. Select **IRDP** from the **Routing > IP > Configuration** group on the Web Agent window. The **ICMP Router Discovery Protocol** dialog box opens (Figure 6-66).

***Figure 6-66. ICMP Router Discovery Protocol Dialog Box***



2. Select the interface on which to enable IRDP in the Select column. A checkmark displays.

3. Refer to Table 6-46 to configure the **ICMP Router Discovery Protocol** dialog box parameters.

*Table 6-46. ICMP Router Discovery Protocol Dialog Box Parameters*

| Parameter | Allows You to... |
|---|---|
| **Select** | Select the interface to be configured. |
| **Interface** | View the IRDP interface name. |
| **Network Address** | View the network IP address of the IRDP interface. |
| **IRDP State** | Select Enable IRDP on the selected interface. The default value is **Disable**. |
| **Preferences** | Enter the preference of the address as a default router address, relative to other router addresses on the same subnet. The minimum value (80000000 hex) is a signed 32-bit value used to indicate that the address should not be used by neighboring hosts as a default router address, even though it may be advertised. The default value is **0**. |
| **Adv. Address** | Select an IP destination address used for multicast router advertisements sent from the interface.<br>Options include:<br>• **Multicast** - Used on any link where listening hosts support IP multicast. The default value is 224.0.0.1.<br>• **Broadcast** - Used on any link where listening hosts support IP unicast. The default value is 255.255.255.255. |
| **Min. Advertisement Interval (sec)** | Enter the minimum time (in seconds) that is allowed between sending unsolicited multicast router advertisements from the interface. This value must be no less than three seconds and no greater than the Max. Advertisement Interval. The default value 450 is **0.75 times the maximum interval**. |
| **Max. Advertisement Interval (sec)** | Enter the maximum time (in seconds) allowed between sending multicast router advertisements sent from the interface. This value must be no less than four seconds and no greater than **1800** seconds. The default value is **600 seconds**. |
| **Advertisement Life Time (sec.)** | Enter the time (in seconds) of the life of a router advertisement that is sent from the interface. This value must be no less than the maximum advertisement interval and no greater than **9000** seconds. The default value is **1800**. |

4. Select **Enable** from the **IRDP State** pull-down menu.

5. Select **Multicast** from the **Adv. Address** pull-down menu.
6. Modify the default value in the **Min. Advertisement Interval (sec.)** field and enter the minimum time interval that passes before the host contacts the switch.
7. Modify the default value in the **Max. Advertisement Interval (sec.)** field and enter the maximum time interval that passes before the host contacts the switch.
8. Modify the default value in the **Advertisement Life Time (sec.)** field, and enter a duration, in seconds, of the IRDP advertisement.
9. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.
10. Select **Global Configuration** from the **Routing > IP > Configuration** group on the Web Agent window. The **IP Global Configuration** dialog box opens (see Figure 6-61).
11. Select **Enable** the **IP Multicast Forwarding** field pull-down menu.
12. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Using the CLI

To enable IRDP on an interface using the CLI, enter the following command in **Enable/Configure/Interface** mode:

```
(config-if:<if name>)# ip irdp
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Configuring Lightweight Directory Access Protocol (LDAP)

LDAP allows you to access the “Access Control Lists”(ACLs), retrieve them from a database on an LDAP server, and apply them to the Avaya P550R/P580/P880/P882 Multiservice switches.

You can also:

- View LDAP statistics for the switch
- Configure a primary and secondary LDAP server
- Configure a search base for the switch to contact in response to an LDAP request.

Configuring a secondary server ensures that LDAP requests can be fulfilled if a primary server fails. The LDAP client sends a search for access control lists to the primary server if the client finds the primary server. The primary server retrieves the access lists from the LDAP database and returns them to the switch’s LDAP client. If the client does not find the primary server and if the primary server does not respond after three retries, the client tries to connect to the secondary server. If the secondary server fails after three retries, the client times out. The LDAP client applies the access lists to manage the way traffic is forwarded.

## Configuring LDAP Settings

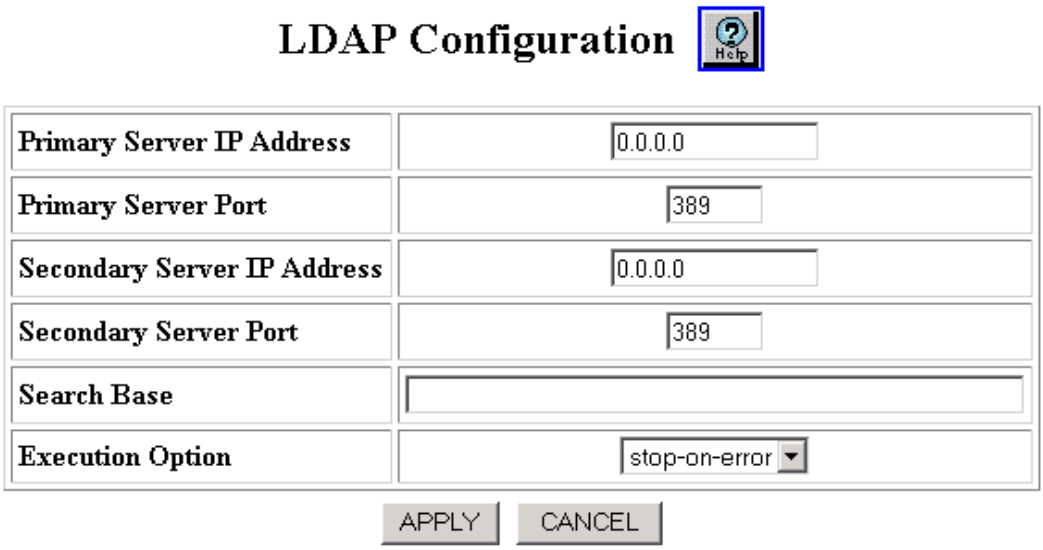
You can configure LDAP settings from either the Web Agent or the CLI.

## Using the Web Agent

To configure LDAP settings from the Web Agent:

1. Select **LDAP Configuration** from the **Routing > IP > Configuration** group on the Web Agent. The **LDAP Configuration** dialog box opens (Figure 6-67).

***Figure 6-67. LDAP Configuration Dialog Box***



2. Refer to Table 6-47 to configure the **LDAP Configuration** dialog box parameters.

*Table 6-47. LDAP Configuration Dialog Box Parameters*

| Parameter | Allows You To... |
|---|---|
| **Primary Server IP Address** | Enter the IP address of your primary LDAP server for the access control list domain. This address is used first when connecting to and downloading access lists from an LDAP server. The default value of 0.0.0.0 indicates to the client that there is no primary LDAP server. |
| **Primary Server Port** | Enter the **port number** of the primary LDAP server for the access control list domain. The port number is used in conjunction with the primary server IP address. There are no special overload values. The default port is 389. |
| **Secondary Server IP Address** | Enter the backup LDAP server IP address for the access control list domain. This address is used as a backup when connecting to and downloading access lists from an LDAP server. If the LDAP client is unsuccessful in connecting to or downloading access lists from the primary server, the secondary server IP address is used. If the primary server IP address has a value of 0.0.0.0, the secondary server IP address is used. The default value is 0.0.0.0.<br>**Note:** Setting the IP address of the secondary server to 0.0.0.0 indicates to the LDAP client that there is no secondary server. |
| **Secondary Server Port** | Enter the backup LDAP server port number for the access control list domain. The port number is used in conjunction with the secondary server IP address. There are no special overload values. The default port number is 389. |
| **Search Base** | Enter the search criteria that will be sent to the LDAP server. The default value is “ou=Devices, ou=AvayaPolicyManager, o=Avaya”.<br>**Note:** No default for the Search Base, this field is empty if the LDAP server has not been installed: |
| **Execution Option** | Open drop-down menu and select **stop-on-error** or **ignore-errors**. This option lets you decide if you want the policy to continue being sent to the device, if LDAP encounters any errors. Select **stop-on-error** if you want execution of the policy to stop on the first error encountered.Select **ignore-errors** if you want execution of the policy to continue even if errors are encountered. In this case, any commands containing errors are ignored. The default value is **stop-on-error.** |

3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Using the CLI

To configure LDAP settings on a primary and secondary server from the CLI, enter the following command from configuration mode:

To Change the LDAP search base, use the following CLI command.

```
<configure># ldap search-base <search-base-DN>
```

To change the primary LDAP server's primary ip address and port, use the following CLI command.

```
<configure># ldap server primary <ip-addr> [<port-
num>]
```

To change the secondary LDAP server's primary ip address and port, use the following CLI command.

```
<configure># ldap server secondary <ip-addr>
[<port-num>]
```

To configure policy retrieval to stop on the first error, or ignore errors, use the following CLI command.

```
<configure># ldap execution-option {stop-on-error
| ignore-errors}
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Viewing LDAP Statistics

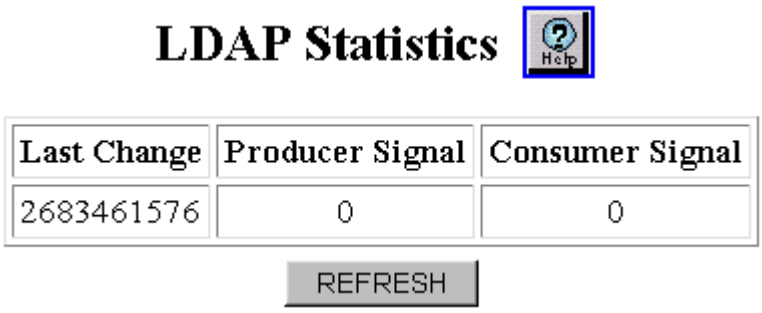
You can view LDAP statistics from either the Web Agent or the CLI.

## Using the Web Agent

To view LDAP statistics using the Web Agent:

1. Select **LDAP Statistics** from the **Routing > IP > Display** group on the Web Agent window. The **LDAP Statistics** dialog box opens (Figure 6-68).

*Figure 6-68. LDAP Statistics Dialog Box*




2. Click **Refresh** to dynamically update **LDAP Statistics** parameters.

3. Refer to Table 6-48 for an explanation of the **LDAP Statistics** dialog box parameters:

*Table 6-48. LDAP Statistics Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Last Change** | Displays the **sysUpTime** since this device was last modified. You can detect a change in the Policy Capabilities by polling a single object using this information. |

*Table 6-48. LDAP Statistics Dialog Box Parameters continued*

| Parameter | Definition |
|---|---|
| **Producer Signal** | The sequence number that, when modified, triggers the LDAP client to download the latest policy from the LDAP server. Typically, Avaya Policy Manager will set this value whenever there is a new policy to download. If this value is a non-zero value, the LDAP client will compare it to the producer signal on the LDAP server. No comparison is made if the value is zero. |
| **Consumer Signal** | Indicates the success of the LDAP client when downloading a policy. If the consumer signal matches the producer signal, downloading LDAP to a policy was successful. If the consumer signal is -1, then either the LDAP client had a problem processing the access lists or the consumer signal set on the LDAP client did not match the signal configured on the LDAP server. If the consumer signal is not -1 and does not match the producer signal, then the LDAP client was unable to connect to the LDAP server(s). |

## Using the CLI

To view configuration and LDAP statistics using the CLI, enter the following command:

```
> show ldap
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

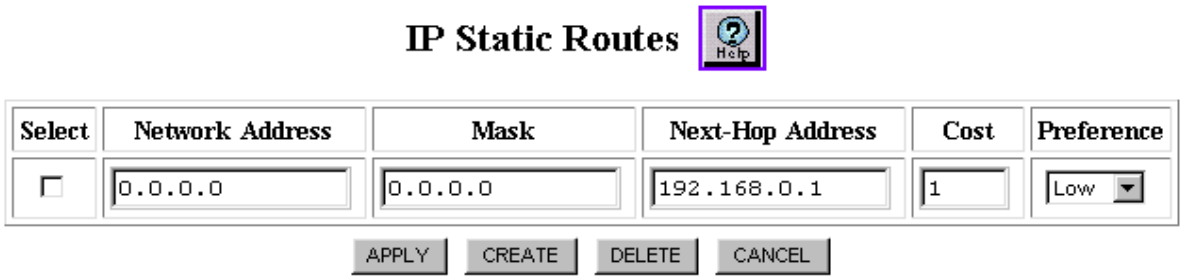
# Configuring a Static Route for the PPP Console

To configure a PPP Console static route:

1. Configure your console serial port as a PPP Console. Refer to the "Connecting a Modem" section in Chapter 2, "*Initialize and Setup*".

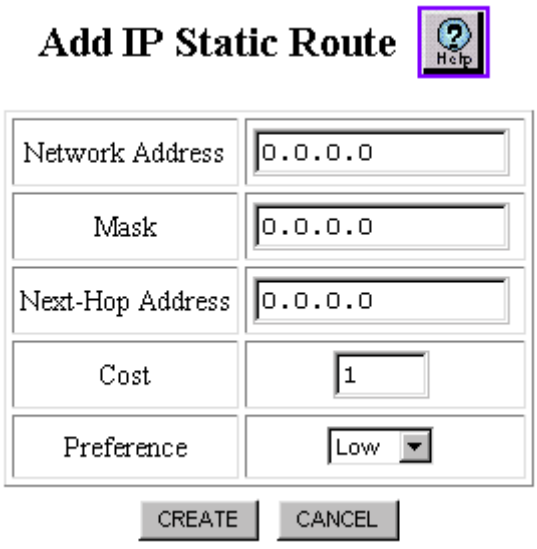
2. Select **Static Routes** from the **Routing > IP > Configuration** folders on the Web Agent window. The I**P Static Routes** dialog box opens (Figure 6-69).

***Figure 6-69. IP Static Routes Dialog Box***




3. Select **CREATE**. The **Add IP Static Routes** dialog box opens (Figure 6-70).

***Figure 6-70. Add IP Static Routes Dialog Box***




4. Enter the IP address that is to be associated with the PPP console port in the Network Address field.

5. Enter the network mask IP address in the **Mask** field.

6. Enter the IP address of the gateway associated with this static route in the **Next-Hop Address** field.
7. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings. The IP Static Routes window re-opens.
8. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

## Configuring the IP Interface for the PPP Console

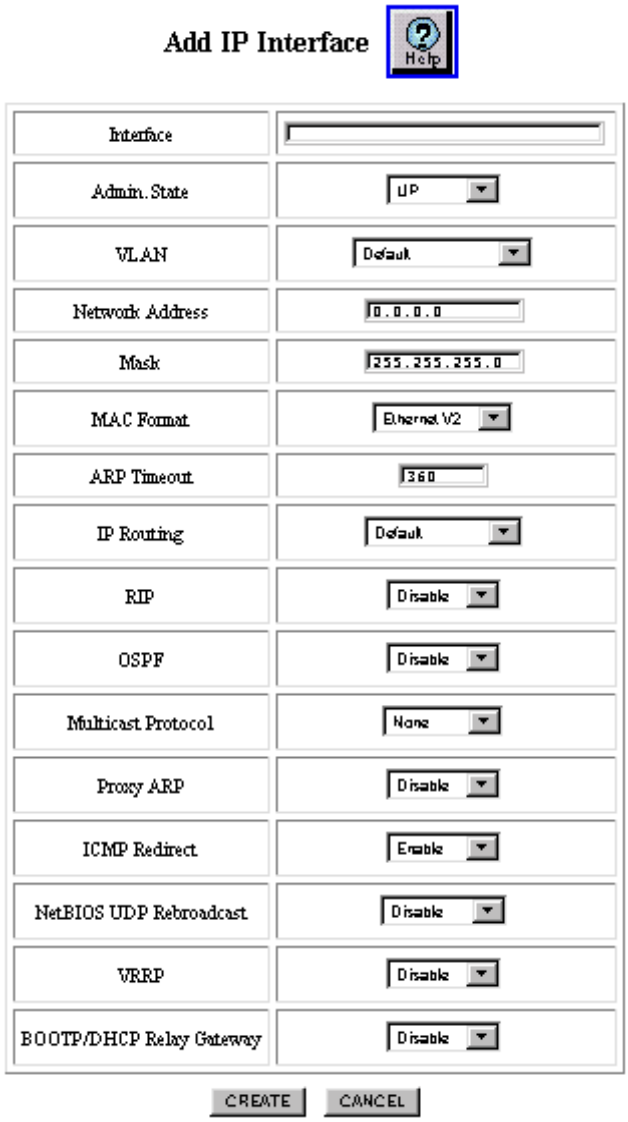
You can configure an IP interface for the PPP console from either the Web Agent or the CLI.

### Using the Web Agent

To configure the PPP console with an IP address and mask using the Web Agent:

1. Configure your console serial port as a PPP Console. See "Connecting a Modem", in Chapter 2, "*Initialize and Setup*".
2. Connect your modem cable to the switch's serial port.
3. Select **Interfaces** from **Routing > IP > Configuration** on the Web Agent window. The **IP Interfaces** dialog box opens (Figure 6-62).
4. Select **CREATE**. The **Add IP Interface** dialog box opens (Figure 6-71).

*Figure 6-71. Add IP Interface Dialog Box*




5. Select **Serial-Console** from the **VLAN** field pull-down menu. This indicates the interface for the PPP console.

6. Enter the IP address in the **Network Address** field that is to be associated with the PPP console port. If you do not enter a name for this interface, the IP address is used.

7. Enter the network mask IP address in the **Mask** field (for example, 255.255.255.0).

8. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings. The IP Interfaces window re-displays.

9. Click **APPLY** to save your changes, or **CANCEL** to clear your selection.

## Using the CLI

To configure the PPP console after you have made all the applicable cable connections with an IP address using the CLI, enter the following command in Interface mode:

```
(config if <interface-name>)# ip VLAN {<VLAN-
id>|name <VLAN-name>| Ethernet-Console|Serial-
Console}
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# 10 Configuring the Routing Information Protocol (RIP)

## Overview

*** Note:** To globally enable RIP, refer to Chapter 9, "Configuring IP Routing".

The information and procedures provided in this chapter pertain to 50 series layer 3, and Licensed 80 series module configurations only:

This section describes:

- Configuring RIP on the Switch
- Modifying RIP Interfaces
- Creating Trusted RIP Neighbors
- Viewing RIP Statistics
- Key Chains
- NBMA IP Interfaces

## Configuring RIP on the Switch

You can configure the RIP from either the Web Agent or the CLI.

*** Note:** MD5 authentication in the 5.*X* versions of switch software is not compatible with MD5 authentication in earlier versions of the software.

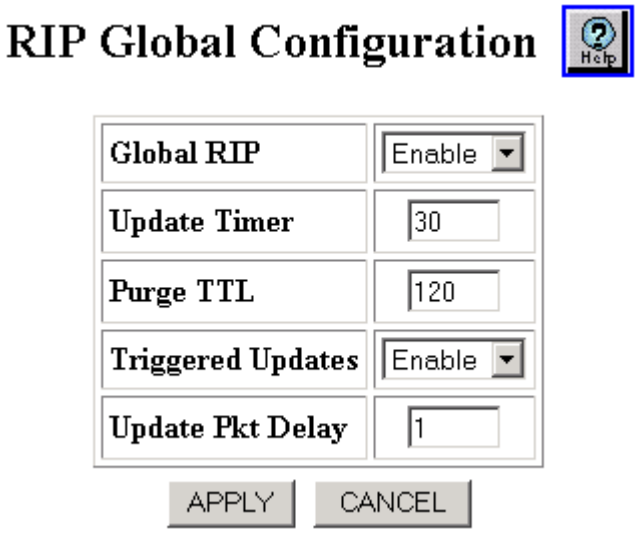
If you enable MD5 authentication on a switch that is running 5.*X* software and on a switch that is running 4.*X* software, the switches do not exchange routing information.

## Configuring RIP on the Switch Using the Web Agent

To configure the RIP globally on your switch using the Web Agent:

1. Select **Global Configuration** from the **Routing > IP > RIP** group on the Web Agent window. The **RIP Global Configuration** dialog box opens (Figure 6-72).

*Figure 6-72. RIP Global Configuration Dialog Box*




2. Refer to Table 6-49 to configure the **RIP Global Configuration** dialog box parameters:

*Table 6-49. RIP Global Configuration Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Global RIP** | Enable or disable the RIP protocol. The default is **Enable.**<br>**Note:** You must disable the IP Interface before Disabling or Enabling RIP. |
| **Update Timer** | Enter the value (in seconds) that represents the time between RIP updates on all interfaces. The parameter range setting is 10-50 ms. The default value is 30 ms. |
| **Purge TTL**<br>**(Garbage Collection Timer)** | Enter the “garbage-collection” time. Upon expiration of the time-out, the route is no longer valid, however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped.Global Time To Live (TTL) in seconds that the RIP update persists. The default value is 120 seconds.The parameter range setting is 1-9999 seconds. |

*Table 6-49. RIP Global Configuration Dialog Box Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **Triggered Updates** | **Disable** or **Enable** route updates that were triggered by a topology change in the network to be added to the routing table. The default is **Enable**. |
| **Update Pkt Delay** | Enter the value (in seconds) that represents the time delay between successive RIP update packets to the neighbor, when the update requires multiple packets. The default value is 1 second. The parameter range setting is 0-50 seconds. |

3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Configuring RIP on the Switch Using the CLI

To configure or modify the RIP parameters globally on your switch using the CLI, enter the following command in router:rip mode:

```
(configure router:rip)# timers basic
<update><invalid>
Update Timer <Msec> <Range:Min=10,Max=50>
(configure router:rip)# output-delay <delay>
(configure router:rip)# triggered updates <CR>
<enable,disable>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about these commands.

# Modifying RIP Interfaces

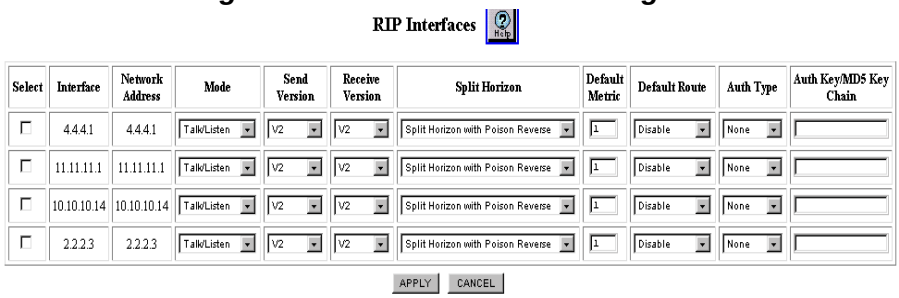
You can modify RIP interfaces from either the Web Agent or the CLI.

## Using the Web Agent

To modify RIP interfaces using the CLI from the Web Agent:

1. Select **Interfaces** from the **Routing > IP > RIP** group on the Web Agent window. The **RIP Interfaces** dialog box opens (Figure 10-2).

***Figure 6-73. RIP Interfaces Dialog Box***




2. Refer to Table 6-50 to modify the **RIP interfaces** dialog box parameters:

***Table 6-50. RIP Interface Dialog Box Parameters***

| Parameter | Allows you to... |
|---|---|
| **Select** | Select the RIP interface to be modified. |
| **Interface** | Displays an interface from a list of interfaces that you previously configured. |
| **Network Address** | Displays an IP address to be associated with the displayed interface. |
| **Mode** | Specify the RIP State. Different states include:<br>• **talk only** (only send RIP information on this interface)<br>• **listen only** (only receive RIP information on this interface)<br>• **talk/listen** (both send and receive RIP information on this interface)<br>**Talk/Listen** is the default setting. |

*Table 6-50. RIP Interface Dialog Box Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **Send Version** | Specify the version of RIP you want to use to send packets across this interface. Selections include:<br>• V1<br>• V2<br>• V1/V2<br>**V1** is the default setting |
| **Receive Version** | Specify the version of RIP you want to use to receive packets. Selections include:<br>• V1<br>• V2<br>• V1/V2<br>**V1** is the default setting |
| **Split Horizon** | Specify that IP routes learned from an immediate neighbor are not advertised back to the neighbor from which the routes were learned.Selections include:<br>• **Split Horizon** - Routes that leave this interface, will not be advertised back on the same interface.<br>• **Split Horizon with Poison Reverse** - Routes that leave this interface, will be advertised back on the same interface with an infinite metric (16). **Split Horizon with Poison Reverse** is the default setting. |
| **Default Metric** | Specify the RIP route metric value. Costing metric used when advertising the RIP route on this interface.<br>**1** is the default setting. The parameter range is 0-15. |
| **Default Route** | Specify the mode for the default route learning on this interface. Different states include:<br>• **Disable** - Disables the default route.<br>• **Talk Only** - Send RIP information to the network.<br>• **Listen Only** - Receive RIP information from the network.<br>• **Talk/Listen** - Both send and receive RIP information from the network.<br>**Disable** is the default setting. |

*Table 6-50. RIP Interface Dialog Box Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **Auth Type** | Specify the type of authentication available for use on a given RIP interface. Authentication types include:<br>• **None** - No authentication required.<br>• **Simple** - Uses a clear-text password for validation. This password is sent unencrypted across the network to neighboring RIP routers.Available for RIP V2 only.<br>• **MD5** - Uses an encrypted **Key** to validate RIP V2 routing updates from neighboring RIP V2 routers.<br>**None** is the default setting |
| **Auth Key** | If **Auth Type** is:<br>• **None** - leave this field blank, or this field is ignored.<br>• **Simple** - Enter the clear-text password for validating RIP packets from neighbor RIP V2 routers.(1-16 characters)<br>• **MD5** - Enter the defined **Key Chain** values under *Routing -> IP-> RIP -> Key Chains*.<br>**None** is the default setting. |

3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Using the CLI

To modify RIP interfaces parameters using the CLI enter the following command from Configure mode:

```
(configure)# interface <intf-name>|[type
{mbna|ethernet}]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Creating Trusted RIP Neighbors

Trusted RIP neighbors enable you to enhance the switch's security by enabling one or more neighbors to relay RIP information.

*** Note:** Adding one or more trusted RIP neighbors ensures that your router accepts only information from these neighbors. Consequently, all other information is filtered. Do not create trusted RIP neighbor(s) if you do not wish to filter RIP information from the network.

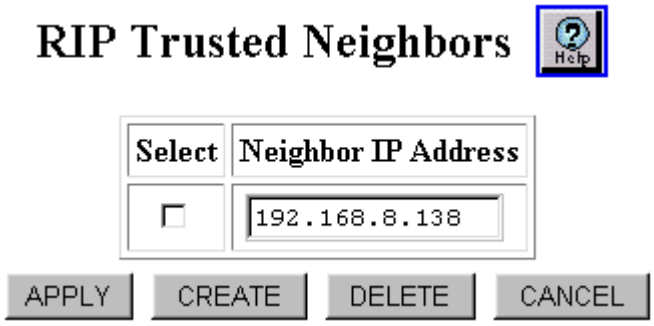
You can create a trusted neighbor using either the Web Agent or the CLI.

## Using the Web Agent

To create a trusted RIP neighbor using the Web Agent:

1. Select **Trusted Neighbors** from the **Routing > IP > RIP** group on the Web Agent window. The **RIP Trusted Neighbors** dialog box opens (Figure 6-74).
2. If a RIP Trusted Neighbor hasn't been configured, only the **CREATE** button appears in Trusted Neighbor Dialog Box.

*Figure 6-74. RIP Trusted Neighbors Dialog Box*




3. Click **CREATE**. The **Add Trusted RIP Neighbor** dialog box opens (Figure 6-75).
4. Click on the Select column checkbox for the Trusted Neighbor and click on **APPLY** to save your changes
5. Click on the Select column checkbox for the Trusted Neighbor and click on **DELETE** to delete the entry or **CANCEL** to restore previous settings.

*Figure 6-75. Add Trusted RIP Neighbors Dialog Box*

6. Enter the IP address for the node that acts as the trusted RIP neighbor in Network Address field.
7. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Creating Trusted RIP Neighbors Using the CLI

To create a trusted RIP neighbor using the CLI enter the following command from **Configure** mode:

```
> (configure)# route rip <cr>
> (configure router rip)# neighbor <ip-addr>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Key Chains

In a full implementation of Key Chains, a **Key Chain** a set of Keys each with its own set of parameters used for MD5 encryption. The parameters are an encryption Key and the period of time that the key is valid. This key must be identical on each device that will participate in an exchange of information. In the case of RIP (version 2 only), routers can use MD5 encryption to ensure that only routing information packets (RIP packets) from authorized routers are accepted.

In a simple implementation, the user creates one Key in a Key Chain and this key is used until it expires.In an advanced implementation, a Key Chain contains multiple keys each valid for a limited amount of time. This provides a periodic change of the encryption key giving the highest level of security. The drawback to this approach is that every device participating in an exchange, such as RIP V2 routers on the same subnet, must have their clocks synchronized. Failure to synchronize would cause devices to use different keys and hence reject RIP updates from neighboring RIP routers.

## Key Chains on the Avaya Multiservice Switch

The Avaya Multiservice switch supports the creation of a single Key Chain with a single Key. Hence, Key and Key Chain are interchangeable terms. The Key has a setting for a start time and duration. Regardless of duration, the Key's start time must be set, ***even if*** the duration is set to infinity.

If the duration is less than 4294967295 seconds, the Key will expire. Ironically, this number is approximately 136 years. A more realistic number would be 18000 seconds (5 Hours). For this time interval, the RIP V2 interface would exchange routes with other RIP V2 routers in the same subnet. Once expired, the RIP V2 interface would no longer accept RIP packets from RIP V2 routers on that subnet.

If the Key's duration is 4294967295 (alternately -1), the key never expires. Again, if you use this value, you must still specify a Key Accept Time. Failure to do so will result in the Avaya switch not creating the Key.

## Configuring the Key Chain using the Web Agent

You can configure Key Chains using the Web Agent or the CLI.

To create a Key Chain/Key using the Web Agent:

1. Select **Key Chain** from the **Routing > IP > RIP** group on the Web Agent window. The **Key Chain** dialog box opens (Figure 6-76.)

***Figure 6-76. Key Chain dialog box***

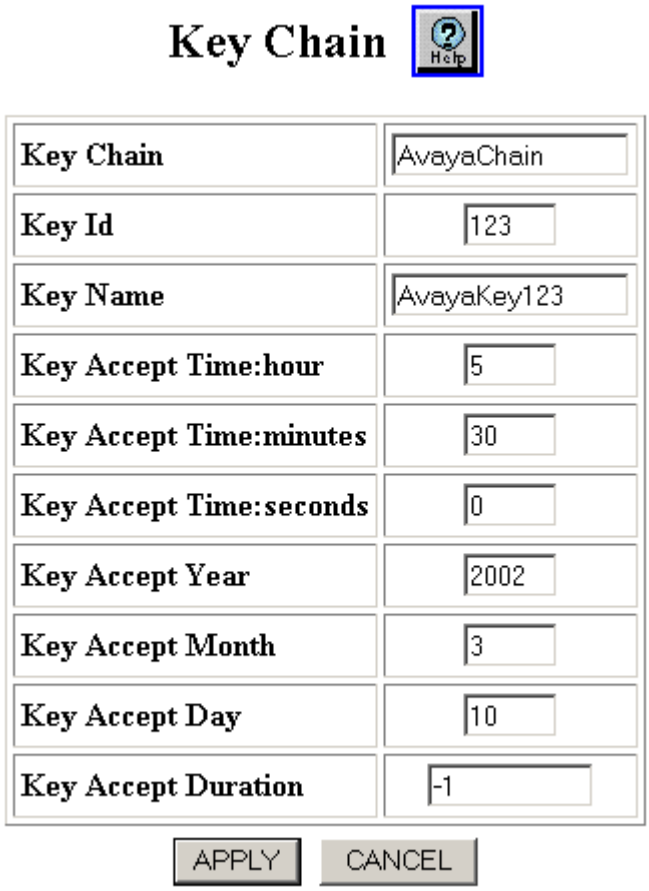


*Table 6-51. Key Chain Parameters*

| Parameter | Defines the... |
|---|---|
| **Key Chain** | 1-16 character ASCII name of the Key Chain |
| **Key ID** | Three digit number of the Key. Valid range 1 to 255. |
| **Key Name** | 16 character alpha-numeric key. This is the actual key used by MD5 encryption. This setting must be identical to the Key on other RIP V2 routers on the same subnet. To be compatible with Cisco devices, do not use a digit (0 - 9) as the first character. |
| **Key Accept Time:hour** | The hour(1-23) this key becomes valid |
| **Key Accept Time:minutes** | The minute(0 - 59) this key becomes valid |
| **Key Accept Time:seconds** | The second(0 - 59) this key becomes valid |
| **Key Accept Year** | The year (2000 - 2009) this key becomes valid |
| **Key Accept Month** | The month (1 - 12) this key becomes valid |
| **Key Accept Day** | The day (1 - 31) this key becomes valid. If you enter a day that does not exist in a month such as the 31st of February, the Key will not be created. |
| **Key Accept Duration** | The duration in seconds that this key is valid. Enter -1 if the key is to last indefinitely. |

2. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Using the CLI

To assignor modify Key Chain parameters using the CLI, enter the following commands from router:rip mode:

To create the Key Chain:

```
(configure router:rip)# key chain <Key Chain>
```

To set the Key Chain ID:

```
(configure router:rip)# key <Key ID>
```

To set the Key Name (MD5 Key):

```
(configure router:rip)# key-string <Key Name>
```

To set the Key Chain's start time and duration:

```
(configure router:rip)# accept-lifetime <hh:mm:ss>
<day> <month> <year> duration {<time> | infinite}
```

### Example of Configuring the Key Chain with the CLI

For Example: To create a **Key Chain** called *AvayaChain* with **Key ID** *123*, **Key Name (**MD5 Key) *AvayaKey123* that begins on March 10, 2002 at 5:30 a.m. and lasts indefinitely, enter the commands in the following order:

```
key chain AvayaChain
key 123
key-string AvayaKey123
accept-lifetime 05:30:00 10 march 2002 duration infinite
```

## Viewing RIP Statistics

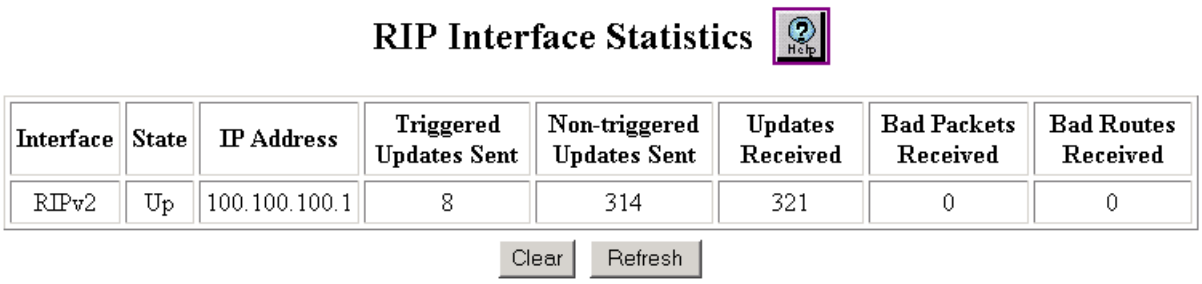
You can view RIP statistics using either the Web Agent or the CLI.

### Viewing RIP Statistics Using the Web Agent

To view RIP statistics using the Web Agent:

1. Select **Interface Statistics** from the **Routing> IP > RIP** group on the Web Agent window. The **RIP Interface Statistics** dialog box opens (Figure 6-77).

***Figure 6-77. RIP Interface Statistics Dialog Box***




2. To modify your RIP statistics:
   - Click CLEAR *to reset all the entries.*
   - Click REFRESH to receive the most up-to-date information on the entries.

**3.** Use Table 6-52 to interpret the RIP statistics:

***Table 6-52. RIP Statistical Parameters***

| Parameter | Defines the... |
|---|---|
| **Interface** | Interface associated with the IP address specified. |
| **State** | Current status of the RIP interface. UP indicates that the interface is up and RIP can transmit and receive updates. |
| **IP Address** | IP address associated with the interface. |
| **Triggered Updates Sent** | Number of RIP triggered updates sent. |
| **Non-Triggered Updates Sent** | Number of RIP non-triggered updates sent. |
| **Updates Received** | Number of RIP updates received based on route changes in the IP routing table. |
| **Bad Packets Received** | Number of bad packets received on this interface. |
| **Bad Routes Received** | Number of bad routes received on this interface. |

## Viewing RIP Statistics Using the CLI

To view RIP statistics using the CLI, enter the following command from Configure mode:

```
> (configure)# show ip rip statistics
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# NBMA IP Interfaces

## Overview

Non-broadcast multi-access (NBMA) functionality was added to RIP and OSPF routing protocols on the Avaya Multiservice switch software. Support for this functionality was added to enable route exchange over nonbridged connections (routed PVCs).For more information about NBMA, refer to the "NBMA IP Interfaces" in Chapter 11, “*Configuring the OSPF Routing Protocol*”.

**CAUTION**

The 5.3.1 NBMA feature is not backward compatible. If you have NBMA interfaces set up and need to downgrade from v5.3.1 to a 5.2 version of software, contact technical support.

# 11 Configuring the OSPF Routing Protocol

## Overview

The following information and procedures provided in this chapter pertain to layer 3 module configuration only:

- What is OSPF?
- Monitoring Switch Performance Using OSPF Statistics
- NBMA IP Interfaces

## What is OSPF?

OSPF (Open Shortest Path First) is a link state networking protocol. Each router broadcasts a packet that describes it own local links. Routers collect information from these broadcast packets to build their own network routing tables. These packets that describe the local links are short and cause less traffic congestion than Routing Information Protocol (RIP), which broadcasts large routing tables.

OSPF bases its routing decision on the least-cost path. The cost is administered value, usually based on line speed. If there are multiple areas in an OSPF domain, there must be a backbone area, identified as **area 0**. When areas are configure in the OSPF domain, there are four basic router classifications:

- Internal Router — router with all directly connected networks belonging to the same area. Routers with only interfaces in the backbone area also belong to this category and have a single link-state database.
- Area Border Router (ABR) — router that has directly connected networks belonging to multiple areas. ABRs have multiple link-state databases, one for each area, including the backbone. ABRs summarize the networks in their areas and advertise them onto the backbone area. The backbone, in turn, distributes the information to the other areas.

- **Backbone Router** — a router that has at lease one directly connected network in the backbone area. This includes all ABRs. However, not all backbone routers must be ABRs. A backbone router that has all its interfaces in the backbone would be an internal backbone router.networks in their areas and advertise them onto the backbone
- **Autonomous System Backbone Router (ASBR**) — router that has directly connected interfaces in non-OSPF networks. These networks are then brought into an OSPF domain. An ASBR is independent of the other router classificiaitons.

*** Note:** The presence of Access Control Lists (ACLs) negatively affects slow path routing.

## Configuring Open Shortest Path First (OSPF)

This section provides the following information about OSPF:


- Configuring the OSPF Global Configuration
- Creating OSPF Areas
- Deleting OSPF Areas
- Modifying OSPF Areas
- Enabling OSPF on an IP Interface
- Modifying OSPF Interfaces
- Creating OSPF Virtual Links
- Deleting OSPF Virtual Links
- Modifying OSPF Virtual Links
- Creating OSPF Summaries
- Deleting OSPF Summaries
- Modifying OSPF Summaries

# Configuring the OSPF Global Configuration

The OSPF global configuration allows you to globally configure OSPF on your switch. It also allows you to specify your router ID and whether or not you want the switch to be the Autonomous System (AS) border router.

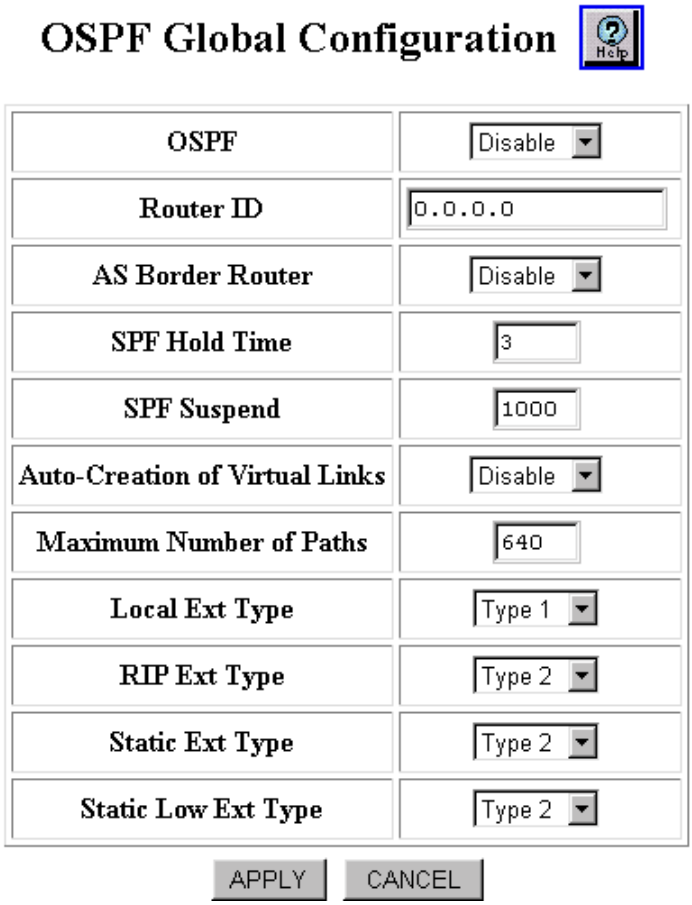
You can globally configure OSPF using either the Web Agent or the CLI.

## Configuring OSPF Globally Using the Web Agent

To globally configure OSPF using the Web Agent:

1. Select **Global Configuration** from the **System > IP > OSPF** group on the Web Agent window. The **OSPF Global Configuration** dialog box opens (Figure 6-78).

***Figure 6-78. OSPF Global Configuration Dialog Box***



2. Refer to Table 6-53 to configure the **OSPF Global Configuration** dialog box parameters:

***Table 6-53. OSPF Global Configuration Dialog Box Parameters***

| Parameter | Allows you to... |
|---|---|
| **OSPF** | Select to enable or disable OSPF globally on your switch. |
| **Router ID** | Specify the Router ID on the switch. The router ID is a 32-bit number assigned to each router running OSPF. This number uniquely identifies the router within an Autonomous System. If 0.0.0.0 is used, the router uses the IP address of an interface. |
| **AS Border Router** | Enable or disable the switch to be an Autonomous System Border Router (ASBR). |
| **SPF Hold Time** | Specify the minimum number of seconds between SPF (shortest path first) runs. |
| **SPF Suspend** | Specify the number of nodes to process SPF runs before suspending. |
| **Auto-Creation of Virtual Links** | Enable or disable the function of automating the creation of virtual circuits based on network topology. This feature is Avaya proprietary and only auto creates virtual links on the config. notes. |
| **Maximum Number of Paths** | Configure the maximum number of paths used when running OSPF. |
| **Local Ext Type** | Specify whether imported local routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics. |
| **RIP Ext Type** | Specify whether imported RIP routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics. |
| **Static Ext Type** | Specify whether imported high preference static routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics. |
| **Static Low Ext Type** | Specify whether imported low preference static routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics. |

3. Click **APPLY** to save changes, or **CANCEL** to restore previous settings.

### Using the CLI

To globally configure OSPF using the CLI, enter the following command in Configure mode:

```
> (configure)# router ospf
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

## Creating OSPF Areas

You can create OSPF areas using either the Web Agent or the CLI.

### Using the Web Agent

To create OSPF areas using the Web Agent:

1. Select **Areas** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Areas** dialog box opens (Figure 6-79).

   *** Note:** The Area ID 0.0.0.0 is a backbone area and always exists in an OSPF configuration.

***Figure 6-79. OSPF Areas Dialog Box***

2. Click **CREATE**. The **Add OSPF Area** dialog box opens (Figure 11-3).

*Figure 6-80. ADD OSPF Area Dialog Box*

3. Refer to Table 6-54 to configure the **Add OSPF Area** dialog box parameters:

*Table 6-54. Add OSPF Area Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Area ID** | Specify the Area ID (32-bit character) for the new area. This must be a unique ID within AS.<br>**Note:** Do not use 0.0.0.0 as an area ID. |
| **Area Type** | Select the type of area. Types include:<br>• **Non-Stub** - Non-edge device/router.<br>• **Stub** - An edge device/router that does not leak external advertisements.<br>• **Not-so-stubby** - This is still a stub area, however, this device/router can leak some external advertisements. |
| **Translate 7 into 5** | **Enable** or **Disable** the translation of the NSSA ASE Type 7 into an AS External LSA Type 5. |
| **Stub Metric** | Specify the stub area default summary cost metric. (Default is 1). |
| **Type 3 ASE Filter** | Select to enable or disable the Type 3 summary LSA filter for Stub and NSSA only. |

4. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

### Creating OSPF Areas Using the CLI

To create OSPF areas using the CLI, enter the following command in **Enable/Configure** mode:

```
> (configure router ospf)# area <area-id> <option>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

*** Note:** If you use the **network area** CLI command to add an interface to an OSPF area, be careful not to enter the IP mask for the <*wildcard-mask*> variable. The <*wildcard-mask*> variable is the inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask.

For example, to enable OSPF on interface 10.10.10.1 (where the network mask is 255.255.255.0) and assign it to area 2.2.2.2, enter:

**network 10.10.10.1 0.0.0.255 area 2.2.2.2**

If you enter the IP network mask (255.255.255.0) instead of the wildcard mask (0.0.0.255), all OSPF interfaces that have 1 for the last octet of their IP address will be added to area 2.2.2.2.

## Deleting OSPF Areas

You can delete an OSPF area using either the Web Agent or the CLI.

### Using the Web Agent

To delete an OSPF area using the Web Agent:

*** Note:** Before deleting an OSPF area, assign any interfaces that are associated with the area to a different area or delete the interfaces.

1. Select **Areas** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Area** dialog box opens (Figure 6-79).
2. Select the OSPF Area to be removed from the **Select** field.
3. Click **DELETE**. The OSPF area you selected is deleted.

### Using the CLI

To delete an OSPF area using the CLI, enter the following command in **Enable/Configure** mode:

*** Note:** Before deleting an OSPF area, assign any interfaces that are associated with the area to a different area or delete the interfaces.

```
<configure router: ospf># no area <area-id>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

## Modifying OSPF Areas

You can modify the parameters of an OSPF area using either the Web Agent or the CLI.

### Using the Web

To modify an OSPF area using the Web Agent:

1. Select **Areas** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Areas** dialog box opens (Figure 6-79).
2. Select an OSPF Area to be modified from the **Select** field.
3. Refer to Table 6-54 and modify the OSPF Area dialog box parameters.
4. Click **Apply** to save your changes, or **Cancel** to ignore your changes.

### Using the CLI

To modify an OSPF area using the CLI, enter the following command in **Enable/Configure** mode:

```
>(configure router ospf)# area <area-id> <option>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

# Enabling OSPF on an IP Interface

You can create an OSPF interface using either the web agent or the CLI after you setup a VLAN and create an IP interface.

## Using the Web Agent

After you have set up a VLAN, you must create the IP interface that your VLAN and your subnet will use to communicate. While creating the IP interface, you must assign it to the VLAN. The last step is to enable IP forwarding (Routing) global parameters.

Refer to

To enable OSPF on the IP interface:

1. Administratively bring down the IP interface. Select the down arrow from the **Admin. State** field and select **DOWN**.

   *** Note:** You must bring the IP interface Down to successfully enable OSPF on the IP interface. If you do not, you will get an error message and OSPF will not be enabled.

2. Select the down arrow from the **OSPF** field.
3. Select **Enable**.
4. Administratively bring the IP interface **UP**.

# Modifying OSPF Interfaces

You can modify the parameters on an OSPF interface using either the Web Agent or the CLI.

## Using the Web

To modify an OSPF interface using the Web Agent:

1. In the navigation pane, expand **Routing** > **IP** > **Configuration** folders.
2. Click **Interfaces**.

   The IP Interfaces Web page is displayed in the content pane.

3. Select the **Select** check box for the interface that you want to modify.

4. In the **Admin. State** column for the interface that you want to modify, select **DOWN**.

   This step disables the interface and must be performed before you perform any OSPF modifications.

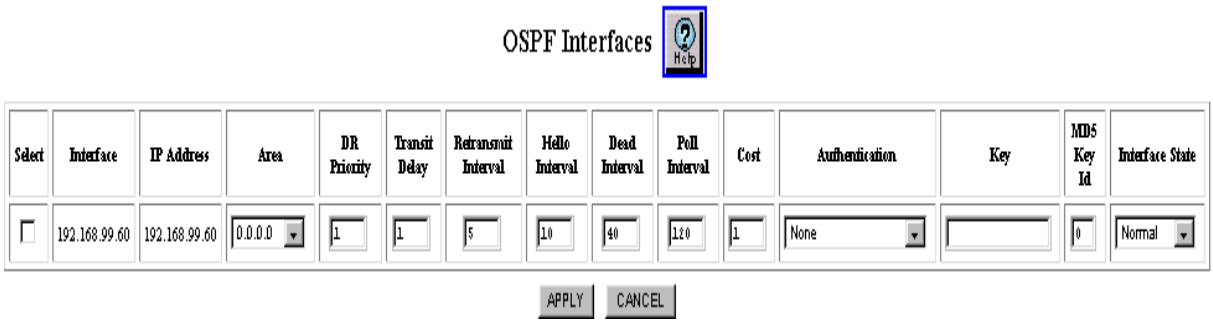
5. Click **Apply**.

6. In the navigation pane, expand the **Routing** > **IP** > **OSPF** folders.

7. Click **Interfaces**.

   The OSPF Interfaces Web page is displayed in the content pane (Figure 11-4).

***Figure 6-81. OSPF Interfaces Dialog Box***




8. Select the **Select** check box for the interface that you want to modify.

9. Modify the OSPF interface as necessary. Refer to Table 6-55 for an explanation of each field on this Web page.

10. Click **Apply**.

11. Reenable the interface:

    a. In the navigation pane, expand **Routing** > **IP** > **Configuration** folders.

    b. Click **Interfaces**.

    The IP Interfaces Web page is displayed in the content pane.

    c. Select the **Select** check box for the interface that you want to reenable.

    d. In the **Admin. State** column for the interface that you want modified, select **UP**.

**e.** Click **Apply**.

*Table 6-55. OSPF Interface Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Select** | Select the OSPF interface to be modified. |
| **Interface** | Displays IP interface (VLAN) that has OSPF enabled.<br>**Note:** This is a read-only field. |
| **IP Address** | Displays IP address associated with the OSPF interface.<br>**Note:** This is a read-only field. |
| **Area** | Enter the area ID configured for this interface. The default is 0.0.0.0. |
| **DR Priority** | Enter the decimal value for this interface for DR priority functionality. The value range is 0-255. The default is 1. |
| **Transmit Delay** | Enter the estimated time (seconds) it takes to transmit a link state update packet over this interface.The value range is 1-3600. The default is 1. |
| **Retransmit Interval** | Enter the time (seconds) between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets. The value range is 1-3600. The default is 5. |
| **Hello Interval** | Enter the time (seconds) between the Hello packets that the router sends on the interface. This value must be the same for all routers attached to a common network. The value range is 1-65535. The default is 10. |
| **Dead Interval** | Enter the time (seconds) that a router's Hello packets have not been seen before it's neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network. The value range is 1-65535. The default is 40. |
| **Poll Interval** | Enter the larger time interval (seconds) between the Hello packets sent to an inactive non-broadcast multiaccess neighbor. he value range is 1-65535. The default is 120. |
| **Cost** | Enter the cost metric associated with this interface. The value range is 1-65535. The default is 1. |
| **Authentication** | Select the type of authentication available for use on a given OSPF interface. Authentication types are:<br>• None (default)<br>• Simple Password<br>• MD5 Authentication |
| **Key** | Enter the authorization key value for the interface. |

*Table 6-55. OSPF Interface Dialog Box Parameters continued*

| Parameter | Definition |
|---|---|
| **MD5 Key ID** | Enter the MD5 authentication key ID as a decimal value. The value range is 1- 255. |
| **Interface State** | Select the interface state. The available sites are:<br>• Normal (default)<br>• Passive |

12. Click **Apply** to save the changes or **Cancel** to ignore the changes

## Using the CLI

To modify an OSPF interface using the CLI, enter the following command:

```
>(configure router ospf)# network <ip-address>
<wildcard-mask><area-id>
```

*** Note:** If you use the **network area** CLI command to add an interface to an OSPF area, be careful not to enter the IP mask for the <*wildcard-mask*> variable.

The <*wildcard-mask*> variable is the inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask.

For example, to enable OSPF on interface 10.10.10.1 (where the network mask is 255.255.255.0) and assign it to area 2.2.2.2, enter:

**network 10.10.10.1 0.0.0.255 area 2.2.2.2**

If you enter the IP network mask (255.255.255.0) instead of the wildcard mask (0.0.0.255), all OSPF interfaces that have 1 for the last octet of their IP address will be added to area 2.2.2.2.

# OSPF Passive-Interface

You can prevent OSPF from sending routing updates across the network by using the **OSPF passive-interface** command. Enabling this command prevents OSPF from sending hello packets across the network. Any OSPF hello packets received from other OSPF routers on the network are also ignored. OSPF advertises the passive-interface as a stub network in the router updates it sends to other OSPF interfaces.

You can set OSPF passive-interface using either the Web Agent or the CLI.

## Using the Web

You can set OSPF passive-interface from the **OSPF Interface** web page. The Interface-State field on the **OSPF Interface** web page can be set to **Passive**, which disables the sending of OSPF routing updates. **Normal**, which enables the sending of OSPF routing updates, is the default.

## Using the CLI

You can set OSPF Passive Interface from the CLI using the commands:

This command defines an OSPF interface as passive-interface.

```
>passive-interface [<interface-name>|
<ip-addr>]
```

This command sets the state of an OSPF interface that is configured as a passive-interface to normal.

```
>no passive-interface [<interface-name>|
<ip-addr>]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

## Using the CLI

To modify an OSPF interface using the CLI, enter the following command from **Configure/Interface** mode:

```
(config-if: <interface>) ip ospf <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

# Creating OSPF Virtual Links

You can create OSPF Virtual links using either the Web Agent or the CLI.

## Creating OSPF Virtual Links Using the Web Agent

To create a OSPF virtual link using the Web Agent:

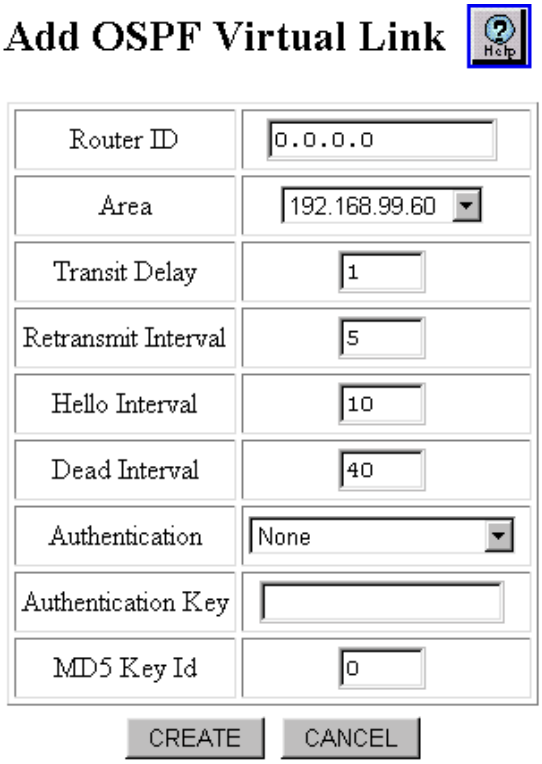
1. Select **Virtual Links** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Virtual Links** dialog box opens (Figure 6-82).

   *** Note:** The OSPF dialog box displays only if OSPF virtual links were previously configured.

***Figure 6-82. OSPF Virtual Links Dialog Box***

2. Select **CREATE**. The **Add OSPF Virtual Link** dialog box opens (Figure 6-83).

*Figure 6-83. Add OSPF Virtual Link Dialog Box*




3. Enter the new OSPF Link information. Refer to Table 6-56 for an explanation of the **Add OSPF Virtual Link** dialog box parameters:

*Table 6-56. Add OSPF Virtual Link Dialog Box Parameters*

| Parameter | Defines the... |
|---|---|
| **Router ID** | Router ID for the far end of the virtual link. |
| **Area** | Area ID through which the virtual link travels. |
| **Transmit Delay** | Estimated number of seconds it takes to transmit a link state update packet over this virtual link. The value range is 1-3600. The default is 1. |
| **Retransmit Interval** | Number of seconds between link-state advertisement retransmissions for adjacencies belonging to this virtual link. This value is also used when retransmitting database description and link-state request packets. The value range is 1-3600. The default is 5. |
| **Hello Interval** | Time in seconds between the Hello packets that the router sends on the virtual link. This value must be the same for all routers attached to a common network. The value range is 1-65535. The default is 10. |

*Table 6-56. Add OSPF Virtual Link Dialog Box Parameters continued*

| Parameter | Defines the... |
|---|---|
| **Dead Interval** | Time in seconds that a router's Hello packets have not been seen before it's neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network.The value range is 1-65535. The default is 40. |
| **Authentication** | Type of authentication available for use on a given OSPF interface. Authentication types include:<br>• None (default)<br>• Simple Password<br>• MD5 Authentication |
| **Authentication Key** | Authentication key for the Area. |
| **MD5 Key ID** | MD5 authentication key ID as a decimal value. The values range is 1-255. |

4. Click **CREATE** to create the virtual link, or **CANCEL** if you do not want to create the OSPF virtual link.

### Using the CLI

To create a OSPF virtual link using the CLI, enter the following command from Configure mode:

```
>(configure router: ospf) area <area-id>
virtual-link <router-id>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

## Deleting OSPF Virtual Links

You can delete OSPF Virtual links using either the Web Agent or the CLI.

### Using the Web Agent

To delete an OSPF virtual link using the Web Agent:

1. Select **Virtual Links** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Virtual Links** dialog box opens (Figure 6-82).
2. Select the virtual link that you want to remove.
3. Click **DELETE**. The virtual link is removed.

### Deleting OSPF Virtual Links Using the CLI

To delete an OSPF virtual link using the CLI, enter the following command from **Enable/Configure** mode:

```
(configure router: ospf)# [no] area <area-id> virtual-link <router-id>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

## Modifying OSPF Virtual Links

You can modify OSPF virtual links using either the Web Agent or the CLI.

### Using the Web Agent

To modify an OSPF virtual link using the Web Agent:

1. Select **Virtual Links** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Virtual Links** dialog box opens (Figure 6-82).
2. Select the virtual link that you want to modify.
3. Refer to Table 6-56 to modify the **OSPF Virtual Links** dialog box parameters.
4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Using the CLI

To modify an OSPF virtual link using the CLI, enter the following command and make your desired changes from Configure mode:

```
(configure router: ospf)# area <area-id> virtual-link <router-id> [hello-interval <seconds>] [retransmit-interval <seconds>] [dead-interval <seconds>] [{authentication-key <key> | message-digest-key <key-id> md5 <key>}]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

# Creating OSPF Summaries

The primary purpose of the OSPF summary is route aggregation. Route aggregation is a group range of IP addresses that are linked to a single address.

You can create a new OSPF summary from either the Web Agent or the CLI.

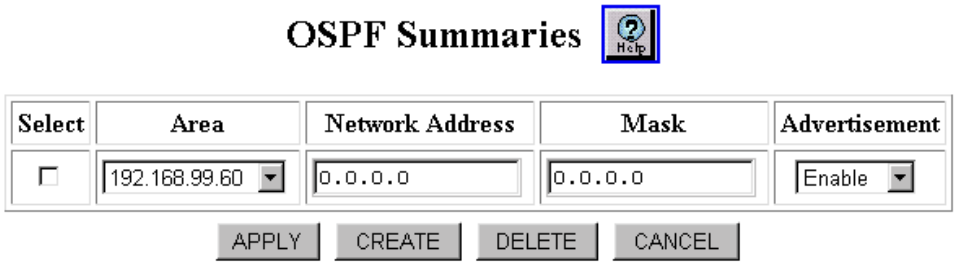
## Using the Web Agent

To create a new OSPF summary using the Web Agent:

1. Select **Summaries** from the **Routing > IP > OSPF** group on the Web Agent window,. The **OSPF Summaries** dialog box opens (Figure 6-84).

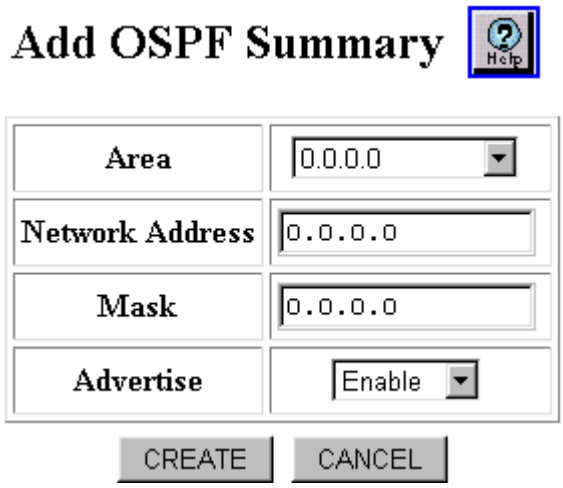
   *** Note:** This dialog box will display OSPF summaries only if you have previously configured one or more summaries.

***Figure 6-84. OSPF Summaries Dialog Box***




2. Select **CREATE**. The **Add OSPF Summary** dialog box opens (Figure 6-85).

*Figure 6-85. Add OSPF Summary Dialog Box*




3. Refer to Table 6-57 for details about the **Add OSPF Summary** dialog box parameters:

*Table 6-57. Add OSPF Summary Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Area** | Select the area ID of the area from which the routes are aggregated (summary IP address). |
| **Network Address** | Enter the IP address of the network to be advertised. |
| **Mask** | Enter the subnet mask of the network to be advertised. |
| **Advertise** | Select the ability to suppress (disable) or enable advertisements of this summary. When suppressing, advertisements of IP routes in this range are also suppressed. |

4. Click **CREATE** to save the new OSPF summary, or **CANCEL** to ignore the new summary.

## Using the CLI

To create a new OSPF summary using the CLI, enter the following command from Configure mode:

```
<configure router: ospf># area <area id> range
<ip address><mask><no-advertise>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

## Deleting OSPF Summaries

You can delete OSPF summaries using either the Web Agent or the CLI.

### Using the Web Agent

To delete an OSPF summary using the Web Agent:

1. Select **Summaries** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Summaries** dialog box opens (Figure 6-84).
2. Select the OSPF summary that you want to remove.
3. Click **DELETE**. The OSPF summary you selected is removed.

### Using the CLI

To delete an OSPF summary using the CLI, enter the following command from Configure mode:

```
(configure router: ospf)# [no] area
<area-id> range <ip-address> <mask>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

## Modifying OSPF Summaries

You can modify an OSPF summary using wither the Web Agent or the CLI.

### Using the Web Agent

To modify an OSPF summary using the Web Agent:

1. Select **Summaries** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Summaries** dialog box opens (Figure 6-84).
2. Select the OSPF summary to be modified.
3. Refer to Table 6-57 to configure the **OSPF Summaries** dialog box parameters.
4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Using the CLI

To modify an OSPF summary using the CLI, enter the following command in **Configure** mode:

```
(configure router: ospf)# area <area-id> range
<ip-address> <mask>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

# Monitoring Switch Performance Using OSPF Statistics

You can monitor switch performance using the following OSPF statistics:

- OSPF Links
- OSPF Neighbors
- OSPF Link Database

## Displaying OSPF Statistics

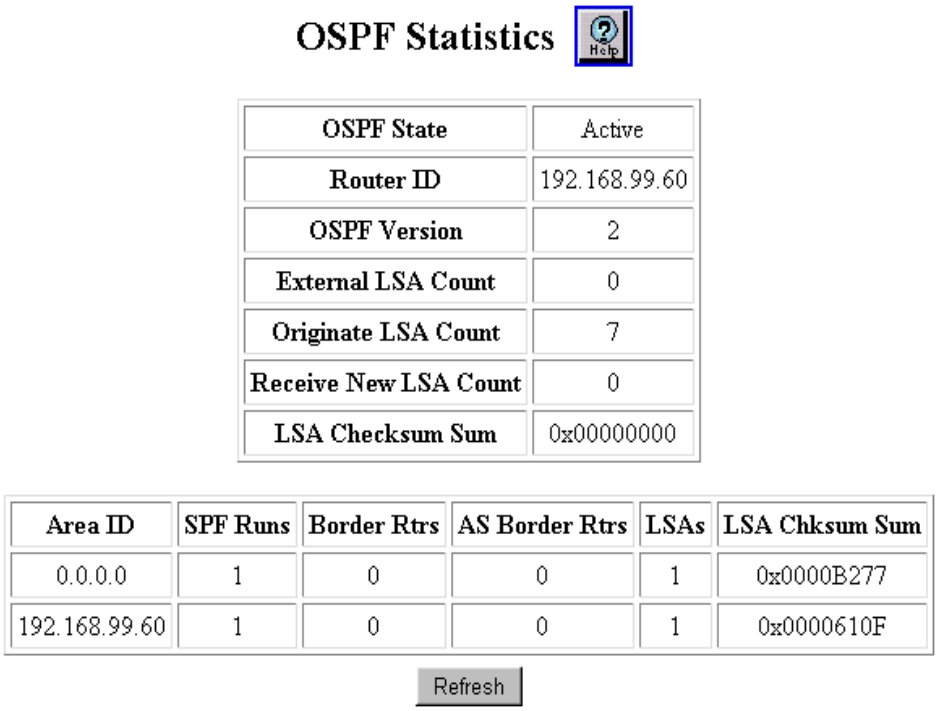
You can display OSPF statistics using either the Web Agent or the CLI.

### Using the Web Agent

To display the OSPF global statistics using the Web Agent:

1. Select **Statistics** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Statistics** dialog box opens (Figure 6-86).

*Figure 6-86. OSPF Statistics Dialog Box*




2. Refer to Table 6-58 for an explanation of the **OSPF Statistics** dialog box parameters:

*Table 6-58. OSPF Statistical Parameters*

| Parameter | Displays the... |
|---|---|
| **OSPF State** | Current state of OSPF. |
| **Router ID** | Router ID for OSPF. |
| **OSPF Version** | Current version of OSPF. The P580/P882 with Integrated Routing supports OSPFv2. |
| **External LSA Count** | Number of external (LS type 5) link state advertisements (LSAs) in the link-state database. |
| **Originate LSA Count** | Number of LSAs originated by this router. |
| **Receive New LSA Count** | Number of new LSAs received by this router. |
| **LSA Checksum Sum (global OSPF system)** | 32-bit unsigned sum of the LS checksums of the external link-state advertisements contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers. |

*Table 6-58. OSPF Statistical Parameters continued*

| Parameter | Displays the... |
|---|---|
| **Area ID** | Area ID of the area in question. It has the function of defining a summarization point for Link State Advertisements. |
| **SPF Runs** | Number of times that the intra-area route table has been calculated using this area's link-state database. |
| **Border Rtrs** | Total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass. |
| **AS Border Rtrs** | Total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass. |
| **LSAs** | Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs. |
| **LSA Chksum Sum (per area, not globally)** | 32-bit unsigned sum of the LS checksums of the external link-state advertisements contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers. |

3. Click **Refresh** to reset the counters with the latest information.

## Using the CLI

To display the OSPF global statistics using the CLI, enter the following command in **Enable** mode:

```
># show ip ospf stats
># show ip ospf virtual-links
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

# Displaying OSPF Links

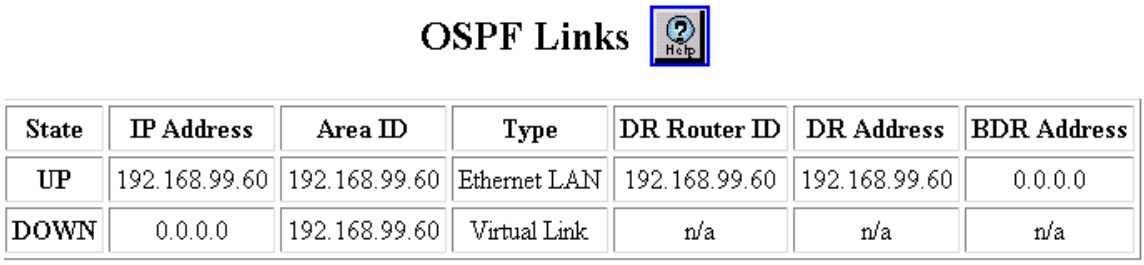
The OSPF link display provides information on the currently active OSPF links. You can display the OSPF using either the Web Agent or the CLI.

## Using the Web Agent

To display OSPF links using the Web Agent:

1. Select **Links** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Links** dialog box opens (Figure 6-87).

***Figure 6-87. OSPF Links Dialog Box***




2. Refer to Table 6-59 for an explanation of the **OSPF Links** dialog box parameters:

***Table 6-59. OSPF Link Parameters***

| Parameter | Displays the... |
|---|---|
| **State** | State of the OSPF link. |
| **IP Address** | IP address of the OSPF link. |
| **Area ID** | Area ID (IP address) associated with the OSPF link. |
| **Type** | Type of OSPF link. |
| **DR Router ID** | Router ID of the designated router. |
| **DR Address** | IP address of the designated router. |
| **BDR Address** | IP address of the designated border router. |

## Using the CLI

To display OSPF links using the CLI, enter the following command from **Enable** mode:

```
>#  show ip ospf interface
>#  show ip ospf virtual-links
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

# Displaying OSPF Neighbors

The OSPF neighbors table summarizes the list of OSPF interfaces and their associated neighbors. You can display OSPF neighbors using either the Web Agent or the CLI.

## Using the Web Agent

To display the OSPF neighbors using the Web Agent:

1. Select **Neighbors** from the **Routing > IP > OSPF** group on the Web Agent window. The **OSPF Neighbors** dialog box opens (Figure 11-11).

***Figure 6-88. OSPF Neighbors Dialog Box***

OSPF Neighbors

| IP Address | State | Router ID | Master | DD Number | DR Priority | E-Option | T-Option | MC-Option | N-Option | OPQ-Option | DR Choice | BDR Choice |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15.0.7.1 | FULL | 15.0.7.1 | Slave | 0x00001107 | 1 | Yes | No | No | No | No | 15.0.7.1 | 15.0.7.2 |
| 15.0.21.2 | FULL | 15.0.21.2 | Master | 0x0000161A | 1 | Yes | No | No | No | No | 15.0.21.2 | 15.0.21.1 |

2. Refer to Table 6-60 to review the **OSPF Neighbors** dialog box parameters:

*Table 6-60. OSPF Neighbors Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **IP Address** | The IP address associated with the OSPF neighbor. |
| **State** | The functional level of an interface. States include:<br>• **Down** - This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor.<br>• **Attempt** - Indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor<br>• **INIT** - Indicates that the Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor.<br>• **2-Way** - Communication between the two routers is bidirectional.<br>• **ExStart** - This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial Database Description sequence number. Neighbor conversations in this state or greater are called adjacencies.<br>• **Exchange** - Router is describing its entire link state database by sending DD (Database Description) packets to the neighbor.<br>• **Loading** - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.<br>• **Full** - The neighboring routers are fully adjacent. These adjacencies appears in router-LSAs and network-LSAs. |
| **Router ID** | The router ID of the neighbor. |
| **Master** | The state of the neighbor: master or slave. |
| **DD Number** | The hexadecimal number used to sequence the collection of Database Description Packets. The initial value (indicated by the Init bit being set) should be unique. The DD sequence number then increments until the complete database description has been sent. |

*Table 6-60. OSPF Neighbors Dialog Box Parameters continued*

| Parameter | Definition |
|---|---|
| **DR Priority** | Displays the DR Priority of the neighboring router.<br>This is used to determine whether this neighbor is eligible to become the *Backup* Designated Router. If 0, the router is ineligible to become the Backup Designated Router. |
| **E-Option** | The method used to flood AS-external-LSAs. |
| **T-Option** | Specifies whether this neighbor is an ASBR. |
| **MC-Option** | Specifies whether this neighbor supports MOSPF. |
| **N-Option** | Specifies whether this neighbor supports the handling of Type-7 LSAs. |
| **OPQ-Option** | Specifies whether this neighbor supports opaque LSAs (LSA type 9-11). |
| **DR Choice** | Interface IP address of the designated router. |
| **BDR Choice** | Interface IP address of the backup designated router. |

### Using the CLI

To display the OSPF neighbors using the CLI, enter the following command in Priv mode:

```
># show ip ospf neighbor
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

## Searching the OSPF Link State Database

You can search the OSPF kink state database using either the Web Agent or the CLI.

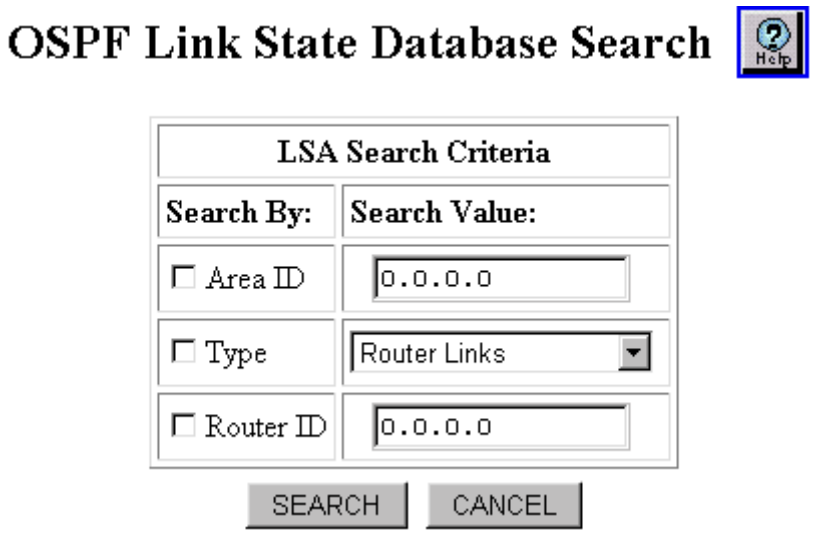
### Searching the OSPF Link State Database Using the Web Agent

To search the OSPF link state database using the Web Agent:

1. Select **Link State Database Search** from the **Routing > IP > OSPF** group on the Web Agent window. The **Link State Database Search** dialog box opens (Figure 6-89).

   *** Note:** You can select more than one item in the **Search By** column to help narrow your search results.

*Figure 6-89. Link State Database Search Dialog Box*




**2.** To search by:

- **Area ID** — click the Area ID checkbox and specify the IP address of the Area ID that you want to find in the database, and click SEARCH.
- **Type** — click the Type checkbox and from the Type pull-down menu, select the type of search you want to perform, and click SEARCH.
- **Router ID** — click the Router ID checkbox and specify the router IP address, and click SEARCH.

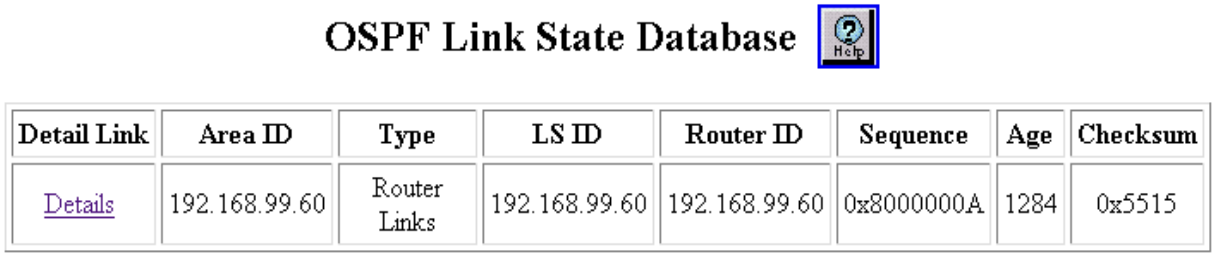
3. Refer to Table 6-61 for an explanation of the **OSPF Link State Database Search** dialog box parameters:

***Table 6-61. OSPF Link State Database Search Dialog Box Parameters***

| Parameter | Allows you to... |
|---|---|
| **Area ID** | Searches the database for the 32-bit identifier of the area from which a LSA was received. |
| **Type** | Searches the database for all entries that match one of the following types:<br>• **Router Links** - These packets describe the states of the router's links to the area and are only flooded within a particular area.<br>• **Network Links** - These packets are generated by Designated Routers and describe the set of routers attached to a particular network.<br>• **Summary Network** - These summaries are generated by Area Border Routers and describe inter-area routes to various networks. They can also be used for aggregating routes.<br>• **Summary AS border** - This describes links to Autonomous System Border Routers and are generated by Area Border Routers.<br>• **AS external** - These packets are generated by Autonomous System Border Routers and describe routes to destination external to the Autonomous system. They are flooded everywhere except stub areas.<br>• **Multicast group** - These packets are generated by multicast groups.<br>• **NSSA external** - These packets are generated by Area Border Routers and describe routes within the NSSA (Not-So-Stubby-Area). |
| **Router ID** | Searches the database for all entries that this router originated. |

4. If your search produces results, the detailed information displays in the OSPF Link State Database dialog box (Figure 6-90).

*Figure 6-90. OSPF Link State Database Dialog Box*




5. Refer to Table 6-62 for an explanation of the **OSPF Link State Database** dialog box parameters.

*Table 6-62. OSPF Link State Database Parameters*

| Parameter | Displays ... |
|---|---|
| **Detail Link** | A link to the LSA Detail dialog box. |
| **Area ID** | The 32-bit identifier of the area from which the LSA was received. |
| **Type** | The LSA format and function. Types include:<br>• **Router Links** - These packets describe the states of the router's links to the area and are only flooded within a particular area.<br>• **Network Links** - These packets are generated by Designated Routers and describe the set of routers attached to a particular network.<br>• **Summary Network** - These summaries are generated by Area Border Routers and describe inter-area routes to various networks. They can also be used for aggregating routes.<br>• **Summary AS Border** - This describes links to Autonomous System Border Routers and are generated by Area Border Routers.<br>• **AS External** - These packets are generated by Autonomous System Border Routers and describe routes to destinations external to the Autonomous system. They are flooded everywhere except stub areas.<br>• **Multicast Group** - These packets are generated by multicast groups.<br>• **NSSA External** - These packets are generated by Area Border Routers and describe routes within the NSSA (Not-So-Stubby-Area). |
| **LS ID** | The piece of routing domain that is being described by the advertisement. Depending on the advertisements LS type, the LS ID displays different values. |

*Table 6-62. OSPF Link State Database Parameters continued*

| Parameter | Displays ... |
|---|---|
| **Router ID** | The 32-bit number that uniquely identifies the originating router in the Autonomous System. |
| **Sequence** | The sequence number. |
| **Age** | Displays the age (in seconds) of the LSA. |
| **Checksum** | Displays the checksum of the complete contents of the advertisement, except the age field. |

6. To update all LSA entries in the database, select **Refresh Table**.

7. To display the details of a specific link state advertisement (LSA), select **Details** from the **Detail Link** column The **LSA Details** dialog box displays with additional search information (Figure 11-14).

*Figure 6-91. LSA Detail Dialog Box*

LSA Detail

| Area | Type | LS ID | Router ID | Sequence | Checksum | Age |
|---|---|---|---|---|---|---|
| 192.168.99.60 | Router Links | 192.168.99.60 | 192.168.99.60 | 0x8000000A | 0x5515 | 1747 |

| Link ID | Link Data | Type | TOS Count | TOS 0 Metric |
|---|---|---|---|---|
| 192.168.99.0 | 255.255.255.0 | Stub Network | 0 | 1 |

8. Refer to Table 6-63 for an explanation of the **LSA Detail** dialog box parameters.

*Table 6-63. LSA Detail Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Area** | Displays the 32-bit identifier of the area from which the LSA was received. |
| **Type** | Displays the link state type. Types include:<br>• Router Links<br>• Network Links<br>• Summary Network<br>• Summary AS Border<br>• AS External<br>• Multicast Group<br>• **NSSA External** |
| **LS ID** | Displays the link-state ID. The link-state ID is an LS type specific field containing either a router ID or an IP address that identifies the piece of the routing domain that is being described by the advertisement. |
| **Router ID** | Displays the router ID of the originator of the link state advertisement. |
| **Sequence** | Displays the link-state sequence number. The sequence number is a 32-bit signed integer. |
| **Checksum** | Displays the checksum of the complete contents of the advertisement, except the age field. |
| **Age** | Displays the time (in seconds) of the LSA. |
| **Network Mask** | Displays the network mask for the LSA. |
| **Attached Router ID 1 &2** | Displays the router ID for the attached router(s). |

9. To update the LSA entry, select **Refresh Entry**.

## Searching the OSPF Link State Database Using the CLI

To search the OSPF link state database using the CLI, enter the following command from Priv mode:

```
>#  show ip ospf database <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3* for details about this command.

# NBMA IP Interfaces

## Overview

Non-broadcast multi-access (NBMA) functionality was added to RIP and OSPF routing protocols on the Avaya Multiservice switch software. Support for this functionality was added to enable route exchange over nonbridged connections (routed PVCs).

This feature makes it possible for the switch to exchange routing information over nonbridged connections (routed virtual switch ports). NBMA functionality has been added to the RIP and OSPF routing protocols in the switch software and has been tested with other routers.

Operation of OSPF over NBMA is almost identical to operation of OSPF over broadcast LANs. Flooding uses the designated router, and both subnets are represented identically within the OSPF link-state database by network-LSAs. The only real difference between broadcast subnets and NBMA subnets is in the discovery of neighboring routers. On broadcast networks, a router can discover its neighbors dynamically by sending multicast Hello packets; on NBMA networks, a router's neighbors may have to be configured.This feature makes it possible for you to set up an IP interface as NBMA. Each IP routing protocol may then have IP addresses that are designated as NBMA neighbors.

Each IP routing protocol may then have IP addresses that are designated as NBMA neighbors. This allows the switch to work with other routers that are routed over PVCs.

**CAUTION**

The 5.3.1 NBMA feature is not backward compatible. If you have NBMA interfaces set up and need to downgrade from v5.3.1 to a 5.2 version of software, contact technical support.

# Setting Up an NBMA IP Interface

You can set up an NBMA IP interface by using either the Web Agent or the Command Line Interface (CLI).

## Using Web Agent

To use the Web Agent to set up an NBMA IP interface:

*** Note:** RIP or OSPF must be enabled to set up NBMA neighbors.

*** Note:** Refer to Chapter 9, “Configuring IP Routing “. to the section called, “Creating and Assigning IP Interface to the VLAN”, for option settings.

1. Open the **Routing** > **IP** > **Configuration** folders.
2. Click **Interfaces**.

   The IP Interfaces Web page opens.
3. Click **Create**.

   The Add IP Interface Web page opens.
4. Enter a name for the interface in the **Name** field.
5. From the **Interface Type** list, select **NBMA**.

   *** Note:** If you enter an IP address to create an NBMA neighbor entry to an interface that is not an NBMA type, the switch will return you to the NBMA Neighbor display page without displaying an error message.
6. Enter the appropriate information in the remaining fields.
7. In either the **RIP** or **OSPF** list or both lists, select **Enable**.
8. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

   *** Note:** You must bring the IP interface Down to successfully enable OSPF on the IP interface. If you do not, you will get an error message and OSPF will not be enabled.

### CLI Commands

To use the CLI to set up an NBMA IP interface:

1. Enter Configuration mode. The CLI displays the following prompt:

   ```
   <configure>#
   ```

For information on how to enter this mode, see "Accessing/Exiting the Command Modes" in Chapter 1, "Overview," of the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3*.

2. Enter the following command at the prompt:

   <configuration># **interface <*interface-name*>**

   The following prompt displays:

   ```
   (configure-if:<interface-name>)#
   ```

3. Enter the following command at the prompt:

   (configure -if: <interface-name>)# **ip address <*ip-addr*> <*mask*>**

4. Enter the following command at the prompt:

   (configure -if: <interface-name>)# **type nbma**

## Setting Up NBMA Neighbors

### Web Agent Procedure

To use the Web Agent to set up NBMA neighbors:

1. Open the **Routing** > **IP** > **RIP** or **OSPF** folders, whichever one was created with an NBMA type interface.
2. Click **NBMA Neighbors**. The RIP or OSPF NBMA Neighbors Web page opens.
3. Click **Create**. The Add NBMA RIP or OSPF Neighbor Web page opens.
4. Enter a neighbor IP interface address in the **Network Address** field.
5. Click **CREATE,** or **CANCEL** to restore previous setting.

### CLI Commands for OSPF

To set up NBMA neighbors on OSPF, you must first create an OSPF interface.

1. After you create an OSPF interface, enter the following command:

   **router ospf**

   The following prompt is displayed:

   `Avaya(configure router:ospf)#`

2. Enter the following command at the prompt:

   **nbma-neighbor** <*ip address*>

To remove the OSPF NBMA neighbor, enter the following command at the `Avaya(configure router:ospf)#` prompt:

no nbma-neighbor <*ip address*>

## Removing NBMA Neighbors

You can remove NBMA neighbors using either the web agent or the CLI.

### Using the Web Agent

To remove the NBMA neighbors using the web agent:

TBD

### Using the CLI

To remove the NBMA neighbors using the CLI, enter the following command at the `Avaya(configure router:rip)#` prompt:

no nbma-neighbor <*ip address*>

*** Note:** Do not change the type of interface after you have created it. If you need to change the interface type, delete the old one and create a new one.

*** Note:** Poll-interval of NBMA interface decreases in value to 0, during the operation. It does not affect the operation of OSPF on an NBMA interface. A panic message will display. Ignore this message.

*** Note:** NBMA RIP2 Poison Reverse in MD5 mode does not advertise all the routes in the Route Table.

RIP2 MD5 Authentication sequence numbers do not persist after you reset the switch.

## CLI Commands for RIP

To set up an NBMA neighbor on RIP, you must first create a RIP interface.

1. After you create a RIP interface, enter the following command at the prompt:

   **router rip**

   The `Avaya(configure router:rip)#` prompt is displayed.

2. Enter the following at the prompt:

   **nbma-neighbor** <*ip address*>

# 12 Configuring IPX Routing

## Overview

This chapter provides the following information and procedures for configuring 50, 80 series layer 2 modules, 50 series Layer 3 or 80 series Licensed Layer 3 modules. Refer to Chapter 1 “Introduction” for more details about routing IP and Internetwork Packet Exchange (IPX) Protocol through the Avaya Multiservice Switch.


- IPX Overview
- Configuring the Avaya Switch as an IPX Router


## IPX Overview

The IPX protocol is connectionless and performs datagram delivery and routing in Novell NetWare networks. Each IPX address consists of:

- **Network Number** — A 32-bit (8 characters) number that is normally assigned by the network administrator.
- **Node Number** — A 48-bit (12 characters) number that is normally the MAC layer address of the physical interface.
- **Socket Number** — A number used to route packets to different processes within the same node.

The syntax for entering an IPX address is:

```
network node socket
```

For example:

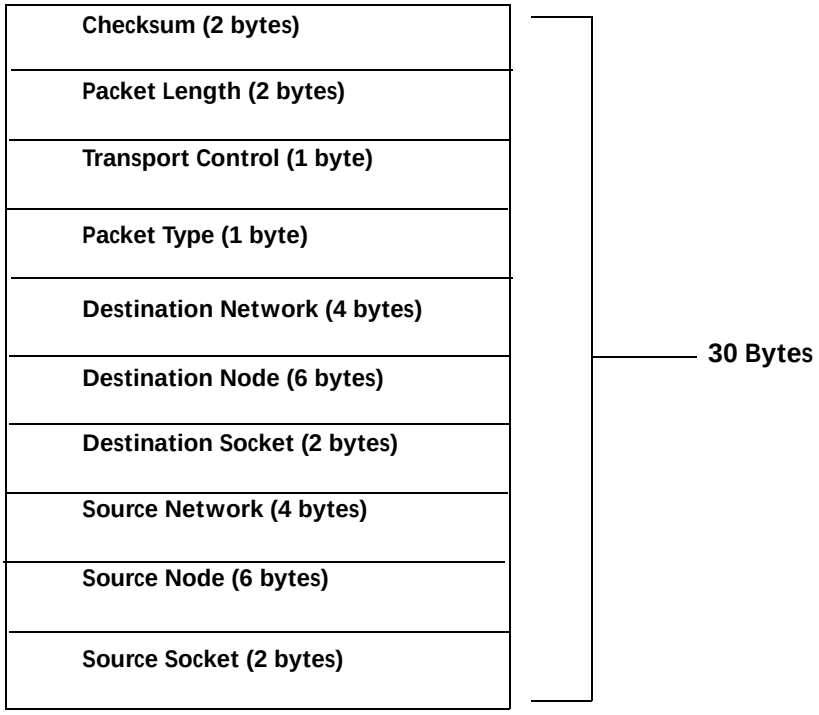
```
000000AAh 00e03b124213h 4003h
```

where `000000AAh` is the network number, `00e03b124213h` is the node number, and `4003h` is the socket number associated with a running process on the end node (for example, RIP, NetWare Link State Protocol (NLSP)).

# IPX Datagram Structure

The IPX datagram contains an IPX header and any data to be transferred on the network. The IPX header is a 30 byte header that contains 10 fields. Figure 6-92 illustrates a conceptual view of an IPX datagram:

***Figure 6-92. IPX Datagram in Detail***




Refer to Table 6-64 for a description of the IPX datagram Structure fields:

***Table 6-64. IPX Datagram Structure Fields***

| Field | Definition |
|---|---|
| **Checksum** | Provides integrity checking.<br>**Note:** Checksum is normally *not enabled* in IPX networks and is usually set to 0xFFFF. |
| **Packet Length** | Length (in bytes) of the packet. |
| **Transport Control** | Number of routers a packet has traversed. This is used to discard a packet if the packet traverses a maximum number of routers (16). |

*Table 6-64. IPX Datagram Structure Fields continued*

| Field | Definition |
|---|---|
| **Packet Type** | Indicates the type of service required or offered by the packet. Types include:<br>• Sequenced Packet Exchange (SPX packet)<br>• NetWare Core Protocol (NCP packet)<br>• NetBIOS (propagated packet) |
| **Destination Network** | The IPX network address of the destination network. |
| **Destination Node** | The MAC address of the destination node. |
| **Destination Socket** | Address of the process running in the destination node. Sockets route packets to different processes within the same node. |
| **Source Network** | The network address of the source network. |
| **Source Node** | The MAC address of the source node. |
| **Source Socket** | Address of the process running in the source node. |

# Configuring the Avaya Switch as an IPX Router

You can configure the Avaya P550R/P580/P880/P882 Multiservice switch as an IPX router. Specific hardware is required to accomplish this configuration.

## Hardware Requirements

To configure your switch as an IPX router, your Avaya P550R/P580/P880/P882 Multiservice switch must be configured with the following hardware:

- 50 Series Layer 3 supervisor module
- Layer 3 50 series media modules.
- 80-Series Supervisor Modules
- 80-Series Licensed Layer 3 media modules

# Configuring IPX Routing Globally

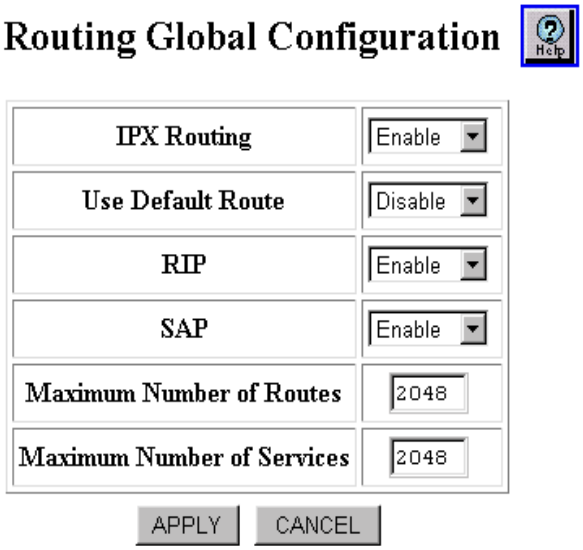
You can configure IPX routing globally using the Web Agent or the CLI.

## Web Agent Procedure

To Enable or Disable IPX routing globally using the Web Agent:

1. Select **Global Configuration** from the **Routing > IPX > Configuration** group on the Web Agent window. The **IPX Global Configuration** dialog box opens (Figure 12-2).

*Figure 6-93. IPX Global Configuration Dialog Box*




2. Configure IPX Routing Global Configuration dialog box parameters to make your switch an IPX router. Refer to Table Table 6-65 for an explanation of the dialog box parameters.

*Table 6-65. IPX Routing Global Configuration Dialog Box Parameters*

| Parameter | Allows you to ... |
|---|---|
| **IPX Routing** | Select Disable to prevent IPX from routing globally. The default value is Enable. |
| **Use Default Route** | Select Enable if you know the default route. The default value is Disable. |
| **RIP** | Select Disable to prevent IPX RIP from routing globally. This affects all IPX interfaces set up to use the IPX RIP routing protocol. The default value is Enable. |
| **SAP** | Select Disable to prevent IPX SAP from routing globally. This affects all IPX interfaces set up to use the IPX SAP routing protocol. The default value is Enable. |

*Table 6-65. IPX Routing Global Configuration Dialog Box Parameters*

| Parameter | Allows you to ... |
|---|---|
| **Maximum Number of Routes** | Enter the maximum number of routes that can be added to the routing table. The switch rounds your entry to the nearest power of 2. For example, if you enter 1000, the system rounds this number up to 1024 routes. The default value is 2048. |
| **Maximum Number of Services** | Enter the maximum number of services that can be added. The switch rounds your entry to the nearest power of 2. For example, if you enter 1000, the system rounds this number up to 1024 services. The default value is 2048. |

3. Click APPLY to save your changes, or CANCEL to restore previous settings.

### CLI Commands

To enable IPX routing globally using the CLI, enter the following command from Configure mode:

```
<configure># ipx routing

To enable IPX routing Globally

<configure> no ipx routing

To disable IPX routing Globally
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Configuring IPX Interfaces

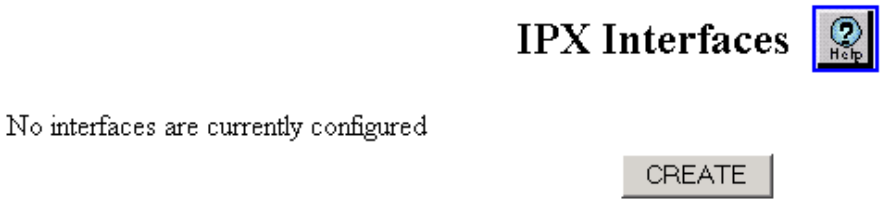
You can create new IPX interfaces and configure up to four interfaces of different encapsulation types to a VLAN (multinetting). You can configure an IPX interface using either the Web Agent or the CLI.

### Web Agent Procedure

To create a new IPX interface using the Web Agent:

1. Select **Interfaces** from **Routing > IPX > Configuration** group on the Web Agent window. The IPX Interfaces dialog box opens (Figure 6-96).

*Figure 6-94. IPX Interfaces Dialog Box*

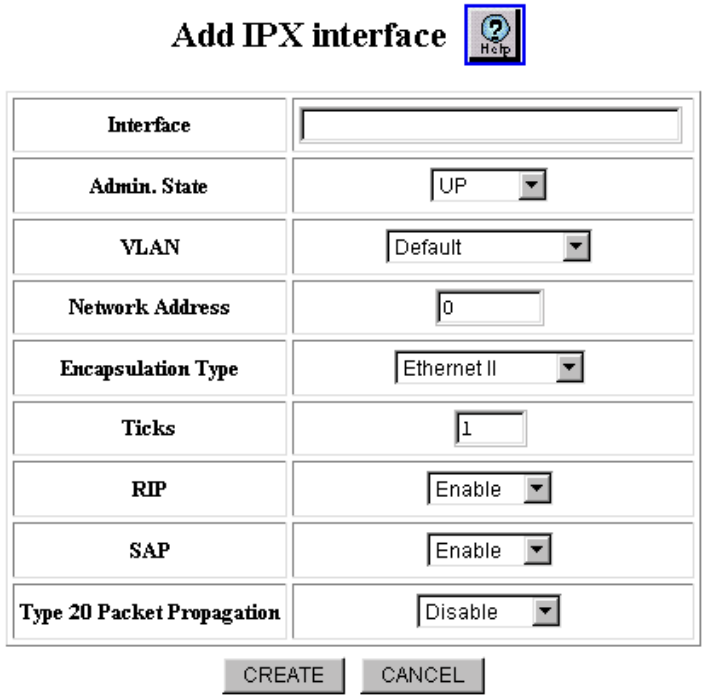



2. To create a new IPX interface Click on **CREATE**

*** Note:** Only the create button is shown if no IPX Interfaces are configured.

3. The **Add IPX interface** Dialog Box opens (Figure 12-4)

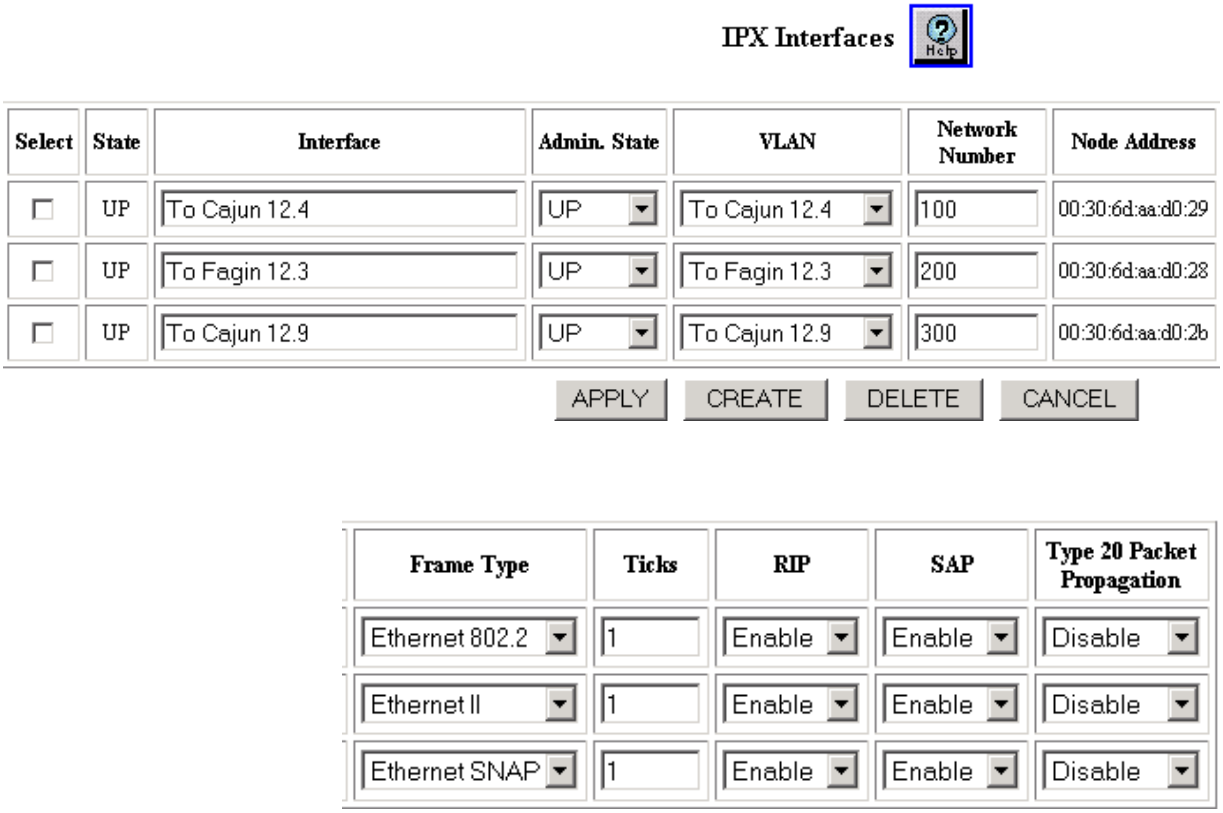
*Figure 6-95. ADD IPX Interface Dialog Box*




4. Refer to Table 12-3 **IPX Interface** to configure an IPX Interface.

5. Select **CREATE**. from the ADD IPX Interface Dialog Box and the **IPX Interface** dialog box opens (see Figure 12-5).

*Figure 6-96. Add IPX Interface Dialog Box*




*** Note:** Due to its length, the **IPX Interfaces** dialog box is split into two views.

6. To view or modify IPX Interfaces, select **IPX Interfaces** from **Routing > IPX > Configuration** group on the Web Agent window. The configured IPX Interfaces dialog box opens (Figure 12-5)

7. Click **APPLY** to save your changes or **CANCEL** to restore previous settings.

*Table 6-66. IPX Interface Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| Select | Select the Interface to be configured. This field id displayed in the IPX Interfaces Dialog box not in the Add Interfaces Dialog box. |
| Admin. State | Select the administration state of the interface.<br>Options include:<br>**Up**<br>**Down** |
| Interface | Enter the name of the IPX interface.Up to 31 Alpha-numeric characters |
| VLAN | Select the VLAN that corresponds to the IPX interface you selected.<br>**Note:** If you need to create a new VLAN, refer to "Creating and Implementing VLANs" in Chapter .4: |
| Network Number | Enter the number of the IPX network you want to assign to the IPX interface. This number is a hexadecimal 32 bit (8 characters) number. |
| Node Address | Displays the node address on which the IPX interface resides. A 48-bit (12 characters) number.<br>This parameter is displayed in the IPX Interface dialog box, not in the Add IPX Interface dialog box. |
| Encapsulation Frame Type | Select the format of the MAC header on the IPX packets sent by the router on the interface. Formats include:<br>**Ethernet II** (Maximum Transmission Unit (MTU) = 1500)<br>**Ethernet 802.2** (MTU = 1497)<br>**Ethernet SNAP** (MTU = 1492)<br>**Ethernet 802.3** (MTU = 1500)<br>The default is **Ethernet II** |
| Ticks | Specify the amount of time (in ticks) that the packet takes to reach the network number you specified. A tick is approximately 1/18th of a second. The default value is **1** |
| RIP | Select Disable to prevent IPX RIP from routing globally. This affects all IPX interfaces set up to use the IPX RIP routing protocol. The default value is **Enable.** |

| Parameter | Allows you to... |
|---|---|
| SAP | Select **Disable** to prevent IPX SAP from routing globally. This affects all IPX interfaces set up to use the IPX SAP routing protocol. The default value is **Enable**. |
| Type 20 Packet Propagation | Specify whether or not Type 20 packets can be sent, received, disabled, or sent and received on a given interface.<br>Options include:<br>**Disable** - Type 20 packets are neither sent nor received.<br>**Inbound** - Type 20 packets are received.<br>**Outbound** - Type 20 packets are sent.<br>**Both** - Type 20 packets are sent and received.<br>The default value is **Disable** |

### CLI Command

To begin the creation of a new IPX interface using the CLI, enter the following command in Configure mode:

```
<configure># interface <interface name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Creating IPX Static Routes

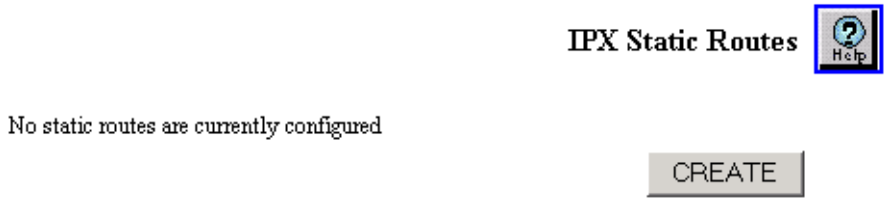
You can create IPX static routes using either the Web Agent or the CLI.

## Web Agent Procedure

To create IPX static routes using the Web Agent:

1. Select **Static Routes** from **Routing > IPX > Configuration** group on the Web Agent window. The IPX Static Routes

***Figure 6-97. IPX Static Routes Dialog Box***




1. dialog box opens (see Figure 12-6)
2. To create a new IPX Static Route Click on **CREATE**

*** Note:** Only the create button is shown if no IPX Static Routes are configured.

3. The **Add IPX Static Route** dialog box opens (see Figure 12-7).

*Figure 6-98. Add IPX Static Route Dialog Box*

4. Refer to Table 6-67 to configure the IPX Static Route parameters.

*Table 6-67. IPX Static Route Parameters*

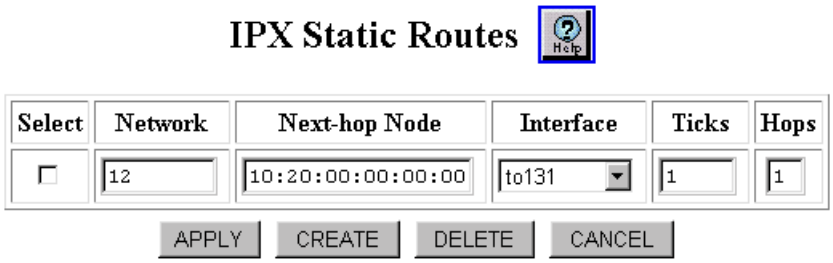
| Parameter | Allows you to ... |
|---|---|
| **Network** | Enter the IPX network number that you want to assign to the IPX static route. |
| **Next-Hop Node** | Enter the MAC address for the next destination to which the packet is routed. Format of the value to enter is **aa:bb:cc:dd:ee:ff**. |
| **Interface** | View the IPX Interface associated with the next hop. |
| **Ticks** | Enter the amount of time (in ticks) that the packet takes to reach the network number you specified. A tick is approximately 1/18th of a second. |
| **Hops** | Enter the number of routers (hops) that the packet must pass through before reaching the network number associated with the IPX network. |

5. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

6. To view or modify IPX Static Routes, select Static Routes from Routing > IPX > Configuration group on the Web Agent window. The configured IPX Static Routes dialog box opens (Figure 12-8)

*** Note:** It is also possible to create a static route by, making a RIP source route from the IPX Static Route Table.

*Figure 6-99. IPX Static Routes Dialog Box*




## CLI Command

To create IPX static routes using the CLI, enter the following command in Interface mode:

```
(config-if:<if-name>)#: ipx route <network
address|range> <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Deleting IPX Static Routes

You can delete an IPX static route using either the Web Agent or the CLI.

## Web Agent Procedure

To delete an IPX static route using the Web Agent:

1. Select **Static Routes** from the **Routing > IPX > Configuration** group on the Web Agent window. The IPX Static Routes dialog box opens (see Figure 12-8).
2. Select the checkbox for the IPX static route that you want to delete from the Select column.
3. Click **DELETE** to remove the IPX static route, or CANCEL to restore the IPX static route.

### CLI Command

To delete an IPX static route using the CLI, enter the following command from Configure mode:

```
(configure)# clear ipx route {<network>
default|*}
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Modifying IPX Static Routes

You can modify IPX static routes form either the Web Agent or the CLI.

### Web Agent Procedure

To modify an IPX static route using the Web Agent:

1. Select **Static Routes** from the **Routing > IPX > Configuration** group on the Web Agent window. The IPX Static Routes dialog box opens (see Figure 6-98).
2. Select the checkbox for the IPX static route that you want to modify from the Select column.
3. Refer to Table 6-67 to modify the IPX Static Route configuration.
4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### CLI Command

To modify an IPX static route using the CLI, enter the following command Interface mode:

```
(config-if:<if-name>)# ipx route <network
address|range> <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Creating IPX Static Services

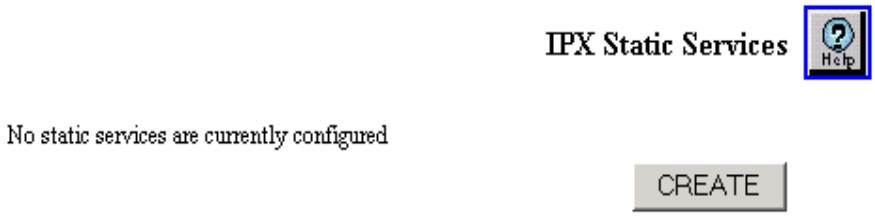
You can create IPX static services using either the Web Agent or the CLI.

## Web Agent Procedure

To create IPX static services using the Web Agent:

1. Select **Static Services** from the **Routing > IPX > Configuration** group on the Web Agent window. The IPX Static Services dialog box opens (see Figure 6-100).

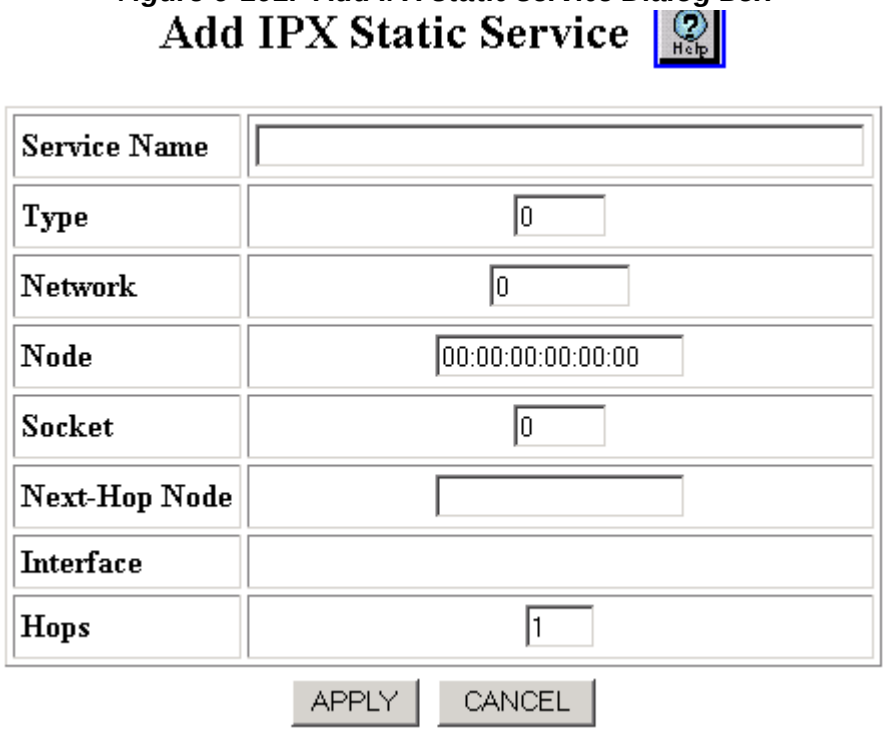
***Figure 6-100. IPX static Services Dialog Box***




2. Select **CREATE** to create a new static service. The **Add IPX Static Service** dialog box opens (see Figure 6-101).

*** Note:** Only the Create button is shown if no IPX Static Services are configured.

***Figure 6-101. Add IPX Static Service Dialog Box***



3. Refer to Table 6-68 to configure the Add IPX Static Service dialog box parameters.

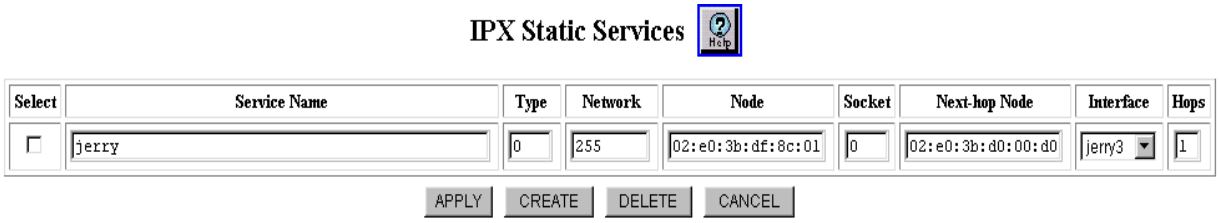
*Table 6-68. IPX Static Service Dialog Box Parameters*

| Parameter | Allows you to ... |
|---|---|
| **Service Name** | Enter the IPX Static Service name. For example, FS_ENG01. Use SLIST (NetWare 3.x) or NLIST (NetWare 4.x) to list your current server names and types from your NetWare server. You may want to explicitly add a service so that clients always use the services of a particular server. |
| **Type** | Enter the service type (in hex) that identifies the type of IPX static service the server provides.<br>Well-known service types include:<br>• Unknown (0)<br>• Print Queue (3)<br>• File Server (4)<br>• Job Server (5)<br>• Print Server (7)<br>• Archive Server (9)<br>• Remote Bridge Server (24)<br>• Advertising Print Server (47) |
| **Network** | Enter the IPX Static Service network number (in Hex). |
| **Node** | Enter the IPX Static Service node address (in hex).<br>The format of the node value is **aa:bb:cc:dd:ee:ff**. |
| **Socket** | Enter the number (in hex) associated with a running process on the end node (for example, RIP, NLSP). |
| **Next-Hop Node** | Enter the MAC address of the next destination through which the service is reached.<br>The format of the node value is **aa:bb:cc:dd:ee:ff**. |
| **Interface** | Enter the interface that corresponds to the next-hop node. |
| **Hops** | Enter the number of routers (hops) that the packet must pass through before reaching the network number associated with the service. |

4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

5. To view or modify IPX Static Services, select **Static Services** from **Routing > IPX > Configuration** group on the Web Agent window. The configured IPX Static Services dialog box opens (Figure 6-102)

*Figure 6-102. IPX Static Services Dialog Box*




### CLI Command

To create IPX static services using the CLI, enter the following command in Configure mode:

```
<configure># ipx service <service-type type
|range>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Deleting IPX Static Service

You can delete an IPX static service using either the Web Agent or the CLI.

### Web Agent Procedure

To delete an IPX static service using the Web Agent:

1. Select **Static Services** from the **Routing > IPX > Configuration** group on the Web Agent window. The IPX Static Services dialog box opens (see Figure 6-100).
2. Select the checkbox for the IPX Static Service that you want to remove.
3. Click **DELETE** to remove the IPX static service, or **CANCEL** to keep the IPX Static Service.

### CLI Command

To delete an IPX static service using the CLI, enter the following command in Configuration mode:

```
(configure)# clear ipx service {<service-type>
<service-name>|*}
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Modifying IPX Static Service

You can modify an IPX static service using either the Web Agent or the CLI.

### Web Agent Procedure

To modify an IPX static service using the Web Agent:

1. Select **Static Services** from the **Routing > IPX > Configuration** group on the Web Agent window. The IPX Static Services dialog box opens (see Figure 6-100).
2. Select the checkbox for the IPX Static Service that you want to modify from the Select column.
3. Refer to Table 6-68 to modify the IPX Static Services dialog box parameters.

### CLI Command

To modify an IPX static service using the CLI, enter the following command in Configure mode:

```
<configure># ipx service <service-type> <service-
name> <network> <node> <socket> <network.next-hop-
node> <hops>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# Monitoring Your Switch Using IPX

This section explains how to use IPX to do the following on your switch:

- Displaying IPX Global Statistics
- Searching the IPX Route Table
- Displaying the IPX Route Table
- Displaying IPX Route Table Statistics
- Searching the IPX Service Table
- Displaying the IPX Service Table
- Displaying IPX Service Table Statistics

# Displaying IPX Global Statistics

IPX Global Statistics count only the IPX packets that are received by or sent from the Supervisor module, not those packets routed in hardware.

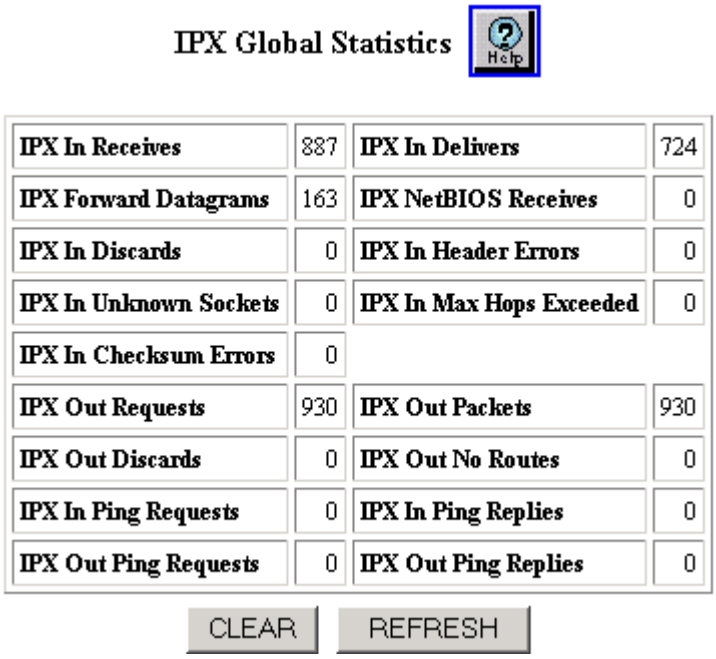
You can display the IPX Global statistics using either the Web Agent or the CLI.

## Web Agent Procedure

To display the global IPX routing statistics using the Web Agent:

1. Select **Global Statistics** from the **Routing > IPX > Display** group on the Web Agent window. The IPX Routing Global Statistics dialog box opens (see Figure 6-103).

***Figure 6-103. IPX Global Statistics Dialogue Box***


IPX Global Statistics
Help
IPX In Receives 887
IPX In Delivers 724
IPX Forward Datagrams 163
IPX NetBIOS Receives 0
IPX In Discards 0
IPX In Header Errors 0
IPX In Unknown Sockets 0
IPX In Max Hops Exceeded 0
IPX In Checksum Errors 0
IPX Out Requests 930
IPX Out Packets 930
IPX Out Discards 0
IPX Out No Routes 0
IPX In Ping Requests 0
IPX In Ping Replies 0
IPX Out Ping Requests 0
IPX Out Ping Replies 0
CLEAR
REFRESH

2. To view the latest statistics available, click **REFRESH** to update all statistics.

3. To reset all of the statistics that are currently displayed, click **CLEAR.** The statistics all reset to zero.

4. Refer to Table 6-69 for a explanation of the IPX Global Statistics dialog box parameters:

*Table 6-69. IPX Global Statistics Dialogue Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **IPX In Receives** | View the total number of IPX packets received (including errors). |
| **IPX In Delivers** | View the total number of IPX packets delivered locally. This includes packets from local applications. |
| **IPX Forward Datagrams** | View the number of IPX packets forwarded. |
| **IPX Netbios Receives** | View the number of NetBIOS packets received. |
| **IPX In Discards** | View the number of IPX packets received but discarded. |
| **IPX In Header Errors** | View the number of IPX packets discarded because of errors in the packet header. This includes packets that are less than the minimum 30 byte length. |
| **IPX In Unknown Sockets** | View the number of IPX packets discarded because the destination socket was not open. |
| **IPX In Max Hops Exceeded** | View the number of IPX packets discarded because the Transport Control field is greater than or equal to 16. |
| **IPX In Checksum Errors** | View the number of IPX packets received with bad checksums. |
| **IPX Out Requests** | View the number of IPX packets supplied locally for transmission. This does not include any packets counted in IPX Forward Datagrams. |
| **IPX Out Packets** | View the total number of IPX packets transmitted. |
| **IPX Out Discards** | View the number of outgoing IPX packets discarded. |
| **IPX Out No Routes** | View the number of IPX packets that cannot be transmitted because no routes are available. |
| **IPX In Ping Requests** | View the number of received ping requests. |
| **IPX In Ping Replies** | View the number of received replies made to ping requests. |
| **IPX Out Ping Requests** | View the number of transmitted ping requests. |
| **IPX Out Ping Replies** | View the number of transmitted replies made to ping requests. |

## CLI Command

To display the global IPX routing statistics using the CLI, enter the following command from Configure mode:

```
<configure># show ipx traffic
```

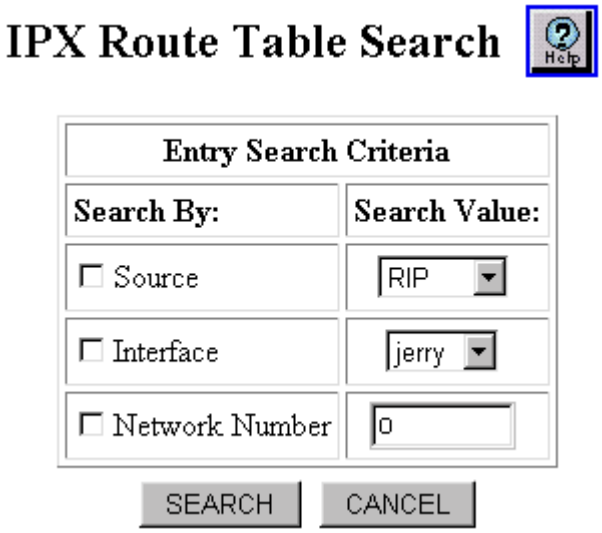
Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Searching the IPX Route Table

To search the IPX route table:

1. Select **Route Table Search** from the **Routing > IPX >** Display Web Agent window. The IPX Route Table Search dialog box opens (see Figure 6-104).

***Figure 6-104. IPX Route Table Search Dialog Box***




2. Select the **SEARCH** Criteria you want to use to find information on specific routes. For example, if you want to find all static routes that are presently configured on your switch, search by source and specify static as your search value.

3. Refer to Table 6-70 to determine the search parameters:

*Table 6-70. IPX Route Table Search Parameters*

| Parameter | Allows you to ... |
|---|---|
| **Source** | Search the IPX route table using of the following parameters:<br>• **RIP** - RIP routing updates<br>• **Static** - User configuration<br>• **Local** - Directly connected routes<br>Once you select a parameter, you can search to find the routes associated with that parameter. |
| **Interface** | Search the IPX Route table using the interface associated with the next-hop to the IPX network. |
| **Network Number** | Search the IPX Route table using the IPX Network address (hexadecimal number) you specify. |

4. Click on the **Search** button to start:

   — If the available routes are found they are displayed in the IPX Route Table dialog box.

   — If no routes are available, a message is displayed in the IPX Route Table dialog box.

## Displaying the IPX Route Table

To display the IPX route table:

1. Perform an IPX Route Table search as described in "Searching the IPX Route Table", section. If available routes are found they are displayed in the IPX Route Table dialog box.

2. Refer to Table 6-71 to review your configuration:

*Table 6-71. IPX Route Table Parameters*

| Parameter | Defines the... |
|---|---|
| **Select** | Parameter selected. |
| **Network** | Network number (in hex) of the IPX network. |
| **Interface** | Interface associated with the IPX network. |
| **Source** | Method by which the network was learned. For example, RIP, local, or static. |
| **TTL** | Number of seconds before the route expires. |

*Table 6-71. IPX Route Table Parameters continued*

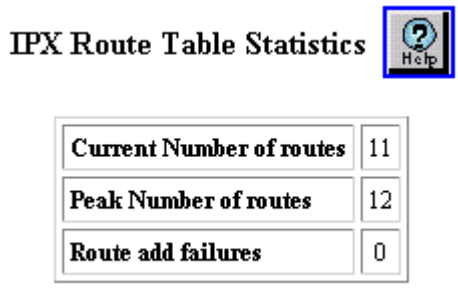
| Parameter | Defines the... |
|---|---|
| **Ticks** | Amount of time (in ticks) that the packet takes to reach the network number you specified. A tick is approximately 1/18th of a second. |
| **Hops** | Number of routers (hops) that the packet must pass through before reaching the network number associated with the IPX network. |
| **Next-Hop MAC Address** | MAC address of the next destination through which the network is reached. |

## Displaying IPX Route Table Statistics

To display your IPX route table statistics:

1. Select **Route Table Statistics** from the **Routing > IPX > Display** Web Agent window. The IPX Route Table Statistics dialog box opens (see Figure 6-105).

*Figure 6-105. IPX Route Table Statistics Dialog Box*




2. Refer to Table 6-72 and review each statistic:

*Table 6-72. IPX Route Table Statistics*

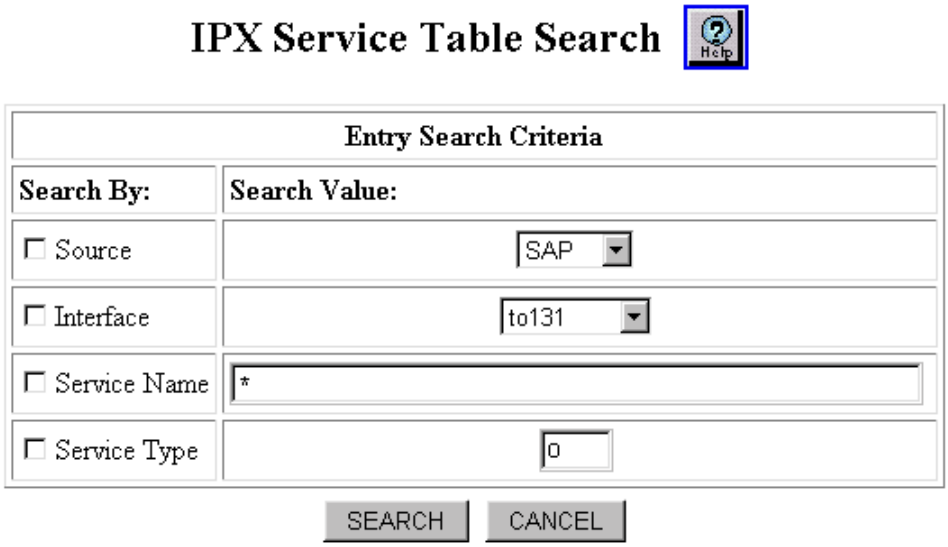
| Statistic | Definition |
|---|---|
| **Current Number of Routes** | Indicates the current number of IPX routes. |
| **Peak Number of Routes** | Lists the peak number of routes. |
| **Route Add Failures** | Indicates the number of failed attempts to add a route to the routing table. |

# Searching the IPX Service Table

To search the IPX service table:

1. Select **Service Table Search** from the **Routing > IPX > Display** Web Agent window. The IPX Service Table Search dialog box opens (see Figure 6-106).

***Figure 6-106. IPX Service Table Search Dialog Box***




2. Select the search criteria you want to use to find information on specific services in the Search By column. For example, if you want to find all static services that are presently configured on your switch, select Source from the Search By column and specify Static as your search value.

3. Refer to Table 6-73 to determine the search parameters:

*Table 6-73. IPX Service Table Search Parameters*

| Parameter | Allows you to ... |
|---|---|
| **Source** | Search the IPX Service Table using one of the following parameters:<br>• **SAP** - Services learned via the SAP protocol<br>• **Static** - User configuration<br>• **Local** - Local services<br>Once you select a parameter, you can search to find the routes associated with that parameter. |
| **Interface** | Search the IPX Service Table using the interface associated with the next-hop to the service. |
| **Service Name** | Search the IPX Service Table using a service name you specify. Note that you can specify a single asterisk (*) to indicate a wildcard character that will match all characters entered before the wildcard. For example, entering FS_ENG* will find all service names that start with FS_ENG. |
| **Service Type** | Search the IPX Service Table using the service type you specify. For example, to specify a print queue type, you would enter 3 (0003h) in the space provided. |

4. Click on the **SEARCH** to start the search.

   — If available services are found they are displayed in IPX Service Table dialog box.

   — If services are not available, a message displays in the IPX Service Table dialog box.

## Displaying the IPX Service Table

To display the IPX service table:

1. Perform an IPX Service table search as described in "Searching the IPX Service Table", earlier in this chapter. If available services are found they are displayed in the IPX Service Table dialog box.

2. Refer to Table 6-74 to review each field in the IPX Services table:

*Table 6-74. IPX Service Table Parameters*

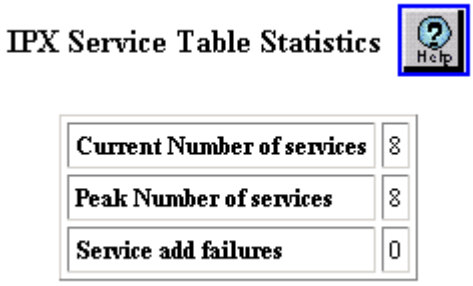
| Parameter | Defines the... |
|---|---|
| **Select** | Parameter selected. |
| **Name** | Name of the service in question. For example, FS_ENG01. (Use SLIST (NetWare 3.x™) or NLIST (NetWare 4.x™) to list your current server names and types from your NetWare server.) |
| **Type** | Service type that identifies the type of service the server provides. Well known service types include:<br>• Unknown (0)<br>• Print Queue (3)<br>• File Server (4)<br>• Job Server (5)<br>• Print Server (7)<br>• Archive Server (9)<br>• Remote Bridge Server (24)<br>• Advertising Print Server (47) |
| **Network** | Network number of the IPX service. |
| **Node** | Node address of the service. |
| **Socket** | Number associated with a running process on the end node (for example, RIP, NLSP). |
| **Interface** | Interface associated with the next hop to the service. |
| **Source** | Method by which the service was learned. For example, SAP or static. |
| **TTL** | Number of seconds before the service expires. |
| **Hops** | Number of routers (hops) that the packet must pass through before reaching the network number associated with the service. |
| **Next-Hop MAC Address** | MAC address of the next destination through which the service is reached. |

## Displaying IPX Service Table Statistics

To display the IPX service table statistics:

1. Select **Service Table Statistics** from the **Routing > IPX > Display** Web Agent window. The IPX Service Table Statistics dialog box opens (Figure 6-107).

*Figure 6-107. IPX Service Table Statistics*




**2.** Refer to Table 6-75 to review each statistic:

*Table 6-75. IPX Service Table Statistics Dialog Box*

| Statistic | Defines the... |
|---|---|
| **Current Number of Services** | The current number of IPX services. |
| **Peak Number of Services** | The peak number of services. |
| **Service Add Failures** | The number of failed attempts to add a service to the routing table. |

# 13 Configuring IPX RIP Protocol

## Overview

The information and procedures provided in this chapter pertain to layer 3 module configuration only. This chapter provides the following procedures:

- Configuring Internetwork Packet Exchange (IPX) Routing Interface Protocol (RIP) Interfaces
- Creating and Modifying IPX RIP Filters

## Configuring Internetwork Packet Exchange (IPX) Routing Interface Protocol (RIP) Interfaces

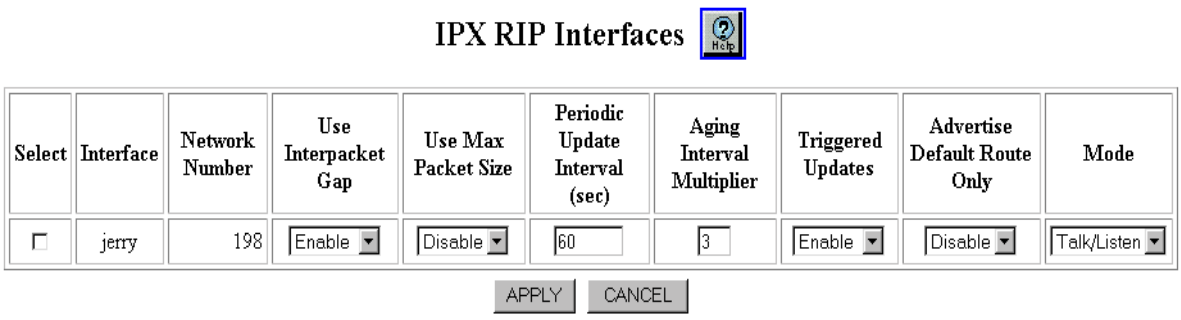
You can configure IPX RIP interfaces using either the Web Agent or the CLI.

### Configuring IPX RIP Interfaces Using the Web Agent

To configure IPX RIP interfaces using the Web Agent:

1. Select **Interfaces** from the **Routing > IPX > RIP** group on the Web Agent window. The **IPX RIP Interfaces** dialog box opens (Figure 6-108). If no IPX interfaces are presently configured then the "No Interfaces are currently configured" message is displayed.

***Figure 6-108. IPX RIP Interfaces Dialog Box***



2. Refer to Table 6-76 to modify the **IPX RIP Interfaces** dialog box parameters:

*Table 6-76. IPX RIP Interfaces Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Select** | Select a RIP interface to modify.<br>**Note:** This field is displayed in the IPX RIP Interface dialog box. |
| **Interface** | Identify the IPX interface associated with the RIP interface. |
| **Network Number** | Identify the number of the IPX network associated with the interface. |
| **Use Interpacket Gap** | Select **Disable** if you do not want RIP updates sent out over an interface to have an interpacket transmission delay. The default is **Enable**. |
| **Use Max Packet Size** | Enable or disable the transmission size of RIP packets sent out an interface:<br>• **If** *enabled*, RIP packets can contain the maximum allowed by the MTU of the RIP interface.<br>• **If** *disabled*, RIP packets are limited to 50 network entries.<br>• The default is **Disabled** |
| **Periodic Update Interval (sec)** | Specify the length of time for the periodic update interval. The default is **60 sec.** |
| **Aging Interval Multiplier** | Specify the length of time that information from received RIP updates are kept as a multiplier of the Periodic Update Interval. The default is **3**. |
| **Triggered Updates** | Select **Disable** to disallow RIP updates to be immediately transmitted to the network in response to changes in the network topology. The default is **Enable**. |
| **Advertise Default Route Only** | Select **Enable** to allow the advertising of the default network exclusively (subject to a route to the default network being known to the switch). The default is **Disable**. |
| **Mode** | Select the one of the following modes for the RIP interface:<br>• **Talk/Listen** - Send and receive advertisements.<br>• **Talk Only** - Send advertisements.<br>• **Listen Only** - Receive advertisements.<br>The default is **Talk/Listen** |

3. Click **APPLY** to save your changes, or CANCEL to restore previous settings.

### Configuring IPX RIP Interfaces Using the CLI

To configure IPX RIP interfaces using the CLI, enter the following command in Interface mode:

```
(config-if: <if name>):# ipx rip
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## Creating and Modifying IPX RIP Filters

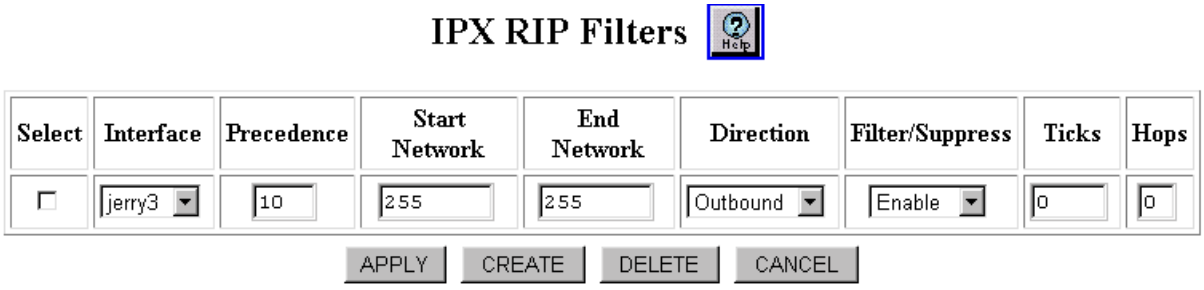
You can create and modify IPX RIP filters from either the Web Agent or the CLI.

### Creating and Modifying IPX RIP Filters Using the Web Agent

To create and modify IPX RIP filters using the Web Agent:

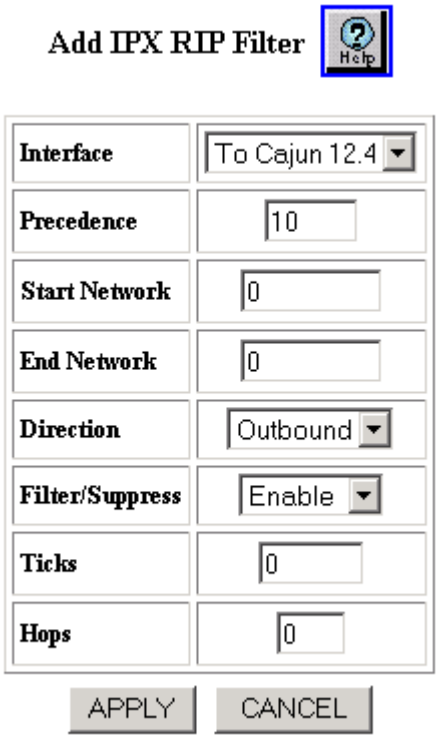
1. Select **Filters** from the **Routing > IPX > RIP** group on the Web Agent window. The **IPX RIP Filters** dialog box opens (Figure 6-109). Only the **CREATE** button is displayed when no filters are configured.

***Figure 6-109. IPX RIP Filters Dialog Box***




2. Select **CREATE** to create a new filter. The **Add IPX RIP Filter** dialog box opens (Figure 6-110).

*Figure 6-110. Add IPX RIP Filter Dialog Box*




3. Refer to Table 6-77 to modify the **Add IPX RIP Filter** dialog box parameters.:

*Table 6-77. Add IPX RIP Filters Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Select** | The Select chechbox selects the IPX Interface. This box only appears with the IPX RIP Filters Dialog Box. |
| **Interface** | Select the interface to which this filter will be applied to RIP packets sent and/or received on the interface. |
| **Precedence** | Specify the filter precedence (in order of importance) with 0 equal to most important.<br>**Note:** All filters on the same interface, must be assigned a unique filter precedence. |
| **Start Network** | Specify the first IPX network number in the range.The default is **0** |
| **End Network** | Specify the last IPX network number in the range.The default is **0** |

*Table 6-77. Add IPX RIP Filters Dialog Box Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **Direction** | Select the direction of the filter from a pull-down menu. The pull-down filter menu options are:<br>• **Inbound** - Apply the filter only to RIP packets received on the interface.<br>• **Outbound** - Apply the filter only to RIP packets sent on the interface.<br>• **Both** - Apply the filter to RIP packets both sent and received on the interface.<br>• The default is **Outbound** |
| **Filter/Suppress** | Disable the IPX networks (within the specified range in the filter) to be filtered (inbound) or suppressed (outbound).<br>• **Filtered** - Apply the filter only to RIP packets received (inbound direction) on the interface.<br>• **Suppressed** - Apply the filter only to RIP packets sent (outbound direction) on the interface.<br>**Enable** allows you to filter and suppress traffic and is the default. Select **Disable** to disable the filtering and suppression of traffic.The default is **Enable** |
| **Ticks** | Specify the time (in ticks) that the packet takes to reach the network number you specified. A tick is approximately 1/18th of a second. This entry is used to override the value in the RIP packet.<br>If you enter **0**, there will be no override in the transmission of data on the network.The default is **o** |
| **Hops** | Specify the number of routers (hops) that the packet must pass through before reaching the network number associated with the IPX interface. This entry is used to override the value in the RIP packet.<br>If you enter **0**, there will be no override in the transmission of data on the network. The default is **0** |

4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Example #1: Configuring your switch to suppress advertising of network 10

To configure your switch to suppress the advertising of network 10 on the IPX interface named Backbone, complete the following steps:

1. Select **Filters** from the **Routing > IPX > RIP** group in the Web Agent window. The **IPX RIP Filters** dialog box opens (Figure 13-3).
2. Select **CREATE** to create a new filter. The **Add IPX RIP Filter** dialog box opens (Figure 6-110).Configure the following parameters on the Add IPX RIP Filter dialog box:
   a. Select **Backbone** from the Interface pull-down menu.
   b. Enter **0** in the **Precedence** field.
   c. Enter **10** in the **Start Network** field.
   d. Enter **10** in the **End Network** field.
   e. Open the **Direction** pull-down menu and select **Outbound**.
   f. Open the **Filter/Suppress** pull-down menu and select **Enable**.
   g. Enter **0** in the **Ticks and Hops** fields.
3. Click **Apply** to save your changes, or **CANCEL** to restore previous settings.

The filter created in this example ensures that all advertising of network 10 from the interface labeled Backbone is suppressed.

**Example #2: Suppress Advertising of all Networks Except 10**

To configure your switch to suppress the advertising of all networks except network 10 on the IPX interface named Backbone, you must first create two filters.

To create filter 1 from the Web Agent:

1. Select **Filters** in the **Routing > IPX > RIP** group on the Web Agent window. The **IPX RIP Filter** dialog box opens (see Figure 6-109).
2. Select **Create** to create a new filter. The **Add IPX RIP Filter** dialog box opens.
3. Configure the following parameters:
   a. Select **Backbone from the Interface pull-down menu.**
   b. Enter **0** in the **Precedence** field.
   c. Enter **10** in the **Start Network** field.

**d.** Enter **10** in the **End Network** field.

**e.** Select **Outbound** from the **Direction** pull-down menu.

**f.** Select **Disable** from the **Filter/Suppress** pull-down menu.

**g.** Enter **0** in the **Ticks and Hops** fields.

Filter 1 ensures that the advertising of network 10 on the interface Backbone will not be suppressed. To suppress all other networks, proceed with the creation of Filter 2.

To create Filter 2 from the Web Agent:

1. Repeat steps 1- 2 in the creating Filter #1 procedure.
2. Configure the following parameters:
   **a.** Select **Backbone** from the **Interface** pull-down menu.
   **b.** Enter **1** in the **Precedence** field.
   **c.** Enter **0** in the **Start Network** field.
   **d.** Enter **ffffffff** in the **End Network** field.
   **e.** Select **Outbound** from the **Direction** pull-down menu.
   **f.** Select **Enable** from the **Filter/Suppress** pull-down menu.
   **g.** Enter **0** in the **Ticks** and **Hops** fields.
3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

Filter 2 ensures that the advertising of all networks on the interface Backbone will be suppressed.

Together, Filter 1 and Filter 2 will act to suppress all network advertising with the *exception* of *network 10*. It is important to note that Filter 2 had the Precedence field set to **1** and Filter 1 had the Precedence field set to **0**. Any filter with a Precedence of 0 will always override a filter with a precedence of 1 or higher.

## Creating and Modifying IPX RIP Filters Using the CLI

To create and modify IPX RIP filters using the CLI, enter the following command from **Configure** mode:

```
<configure># ipx rip-filter <precedence> <start-
network> <end-network> {outbound|inbound|both}
{filter| allow} [<filter-ticks> [<filter-hops>]]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

## View RIP Interface Statistics

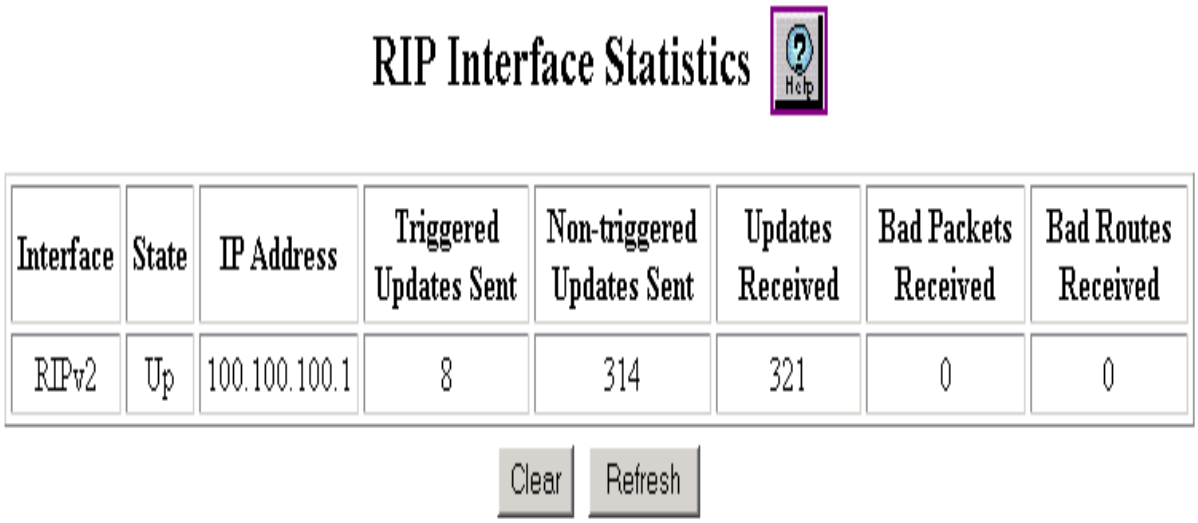
You can view RIP Interface Statistics from either the Web Agent or the CLI.

### Viewing RIP Interface Statistics Using the Web Agent

To view **RIP Interface Statistics** using the Web Agent:

1. Select **Interface Statistics** from the **Routing > IPX > RIP Interface Statistics** group in the Web Agent window. The **RIP Interface Statistics** dialog box opens (Figure 13-4).

***Figure 6-111. IPX RIP Interface Statistics Dialog Box***




2. Refer to Table 13-3 for an explanation of the **IPX RIP interface Statistics**.

3. Click on **CLEAR** to remove the statistics, or **REFRESH** to access current interfaces statistics.

***Table 6-78. IPX RIP Interface Statistical Parameters***

| Parameter | Definition |
|---|---|
| Interface | The IPX interface associated with this RIP interface. |
| State | The current state of the RIP interface. |

*Table 6-78. IPX RIP Interface Statistical Parameters continued*

| Parameter | Definition |
|---|---|
| Network Number | The network number of the IPX network associated with the interface. |
| Triggered Updates Sent | The number of triggered updates sent from the RIP interface. |
| Non-triggered Updates Sent | The number of non-triggered updates sent from the RIP interface. |
| Updates Received | The number of updates received. Updates may be received periodically even if no changes have occurred. |
| Requests Received | The number of requests received on the RIP interface. |
| Bad Packets Received | The number of bad packets received on the RIP interface. |

## Interpreting IPX RIP Interface Statistics Using the CLI

To interpret IPX RIP interface statistics using the CLI, enter the following command from Interface mode:

```
(config-if <interface name>)# show ipx interface
[<intf-name>]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3* for details about this command.

# 14 Configuring IPX SAP Protocol

## Overview

The information and procedures provided in this chapter pertain to layer 3 module configuration only. This chapter provides the following procedures:

- Configuring Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP) Interfaces
- Creating IPX SAP Filters
- Interpreting IPX SAP Interface Statistics

## Configuring Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP) Interfaces

You can configure IPX SAP using either the Web Agent or the CLI.

### Configuring IPX SAP Interfaces Using the Web Agent

To configure the IPX SAP interfaces using the Web Agent:

1. Select **Interfaces** from the **Routing > IPX > SAP** group on the Web Agent window. The **IPX SAP Interfaces** dialog box opens (Figure 6-112). If no IPX interfaces are presently configured then the "No Interfaces are currently configured" message is displayed.

***Figure 6-112. IPX SAP Interfaces Dialog Box***

IPX SAP Interfaces

| Select | Interface | Network Number | Use Interpacket Gap | Use Max Packet Size | Periodic Update Interval (sec) | Aging Interval Multiplier | Triggered Updates | Get Nearest Server Reply | Get Nearest Server Reply Delay (msec) | Mode |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | To Cajun 12.4 | 100 | Enable | Disable | 60 | 3 | Enable | Enable | 0 | Talk/Listen |
| ☐ | To Fagin 12.3 | 200 | Enable | Disable | 60 | 3 | Enable | Enable | 0 | Talk/Listen |
| ☐ | To Cajun 12.9 | 300 | Enable | Disable | 60 | 3 | Enable | Enable | 0 | Talk/Listen |

2. Refer to Table 6-79 to configure the **IPX SAP Interface** dialog box parameters:

*Table 6-79. IPX SAP Interface Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Select** | Select a SAP interface to modify. |
| **Interface** | Identifies the IPX interface associated with the SAP interface. |
| **Network Number** | Identifies the number of the IPX network associated with the interface. |
| **Use Interpacket Gap** | Select one of the following from the pull-down menu:<br>• **Disable –** if you do not want the IPX SAP periodic update packets to be sent out over an interface with no interpacket transmission delay.<br>• **Enable** – If you want to send the IPX SAP periodic update packets to be sent out over an interface with an interpacket transmission delay (default). |
| **Use Max Packet Size** | Select one of the following from the pull-down menu:<br>• **Disable –** To limit SAP packets to 7 service entries(default).<br>• **Enable** – To allow SAP) packets to contain the maximum number of services entries that are allowed by the SAP Interface MTU (default). |
| **Periodic Update Interval (sec)** | Enter (in seconds) the interval at which periodic SAP updates are sent out an interface.Default is 60 seconds. |
| **Aging Interval Multiplier** | Enter the length of time that information from received SAP updates are kept as a multiplier of the Periodic Update Interval.Default is 3. |
| **Triggered Updates** | Select one of the following from the pull-down menu:<br>• **Disable –** To prevent SAP updates from being immediately transmitted to the network in response to changes in the network topology<br>• **Enable** – To allow SAP updates to be immediately transmitted to the network in response to changes in the network topology (default). |

*Table 6-79. IPX SAP Interface Dialog Box Parameters continued*

| Parameter | Allows you to... |
|---|---|
| **Get Nearest Server Reply** | Select one of the following from the pull-down menu:<br>• **Disable –** To prevent the router from responding to **Get Nearest Server** requests received on the interface<br>• **Enable** – To allow the router to respond to **Get Nearest Server** requests received on the interface (default). |
| **Get Nearest Server Reply Delay(msec.)** | Specify the delay (in msecs) to wait before responding to a Get Nearest Service request received on the interface.Default is 0. |
| **Mode** | Select one of the following from the pull-down menu:<br>• **Talk/Listen** - Send and receive advertisements (default).<br>• **Talk Only** - Send advertisements.<br>• **Listen Only** - Receive advertisements. |

3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Configuring IPX SAP Interfaces Using the CLI

To configure the IPX SAP interfaces using the CLI, enter the following command from Interface mode:

```
(config-if <interface-name>):# ipx sap
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Creating IPX SAP Filters

This section provides the following procedures:

- Creating IPX SAP Name Filters
- Creating IPX SAP Network Filters

# Creating IPX SAP Name Filters

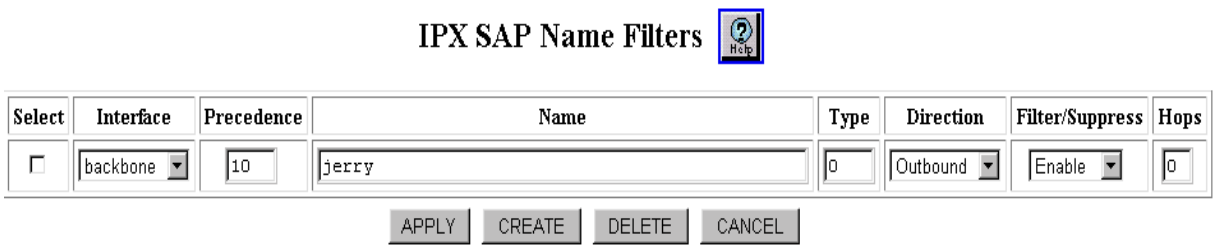
You can create IPX SAP name filter suing either the Web Agent or the CLI.

## Creating IPX SAP Name Filters Using the Web Agent

To create IPX SAP name filters using the Web Agent:

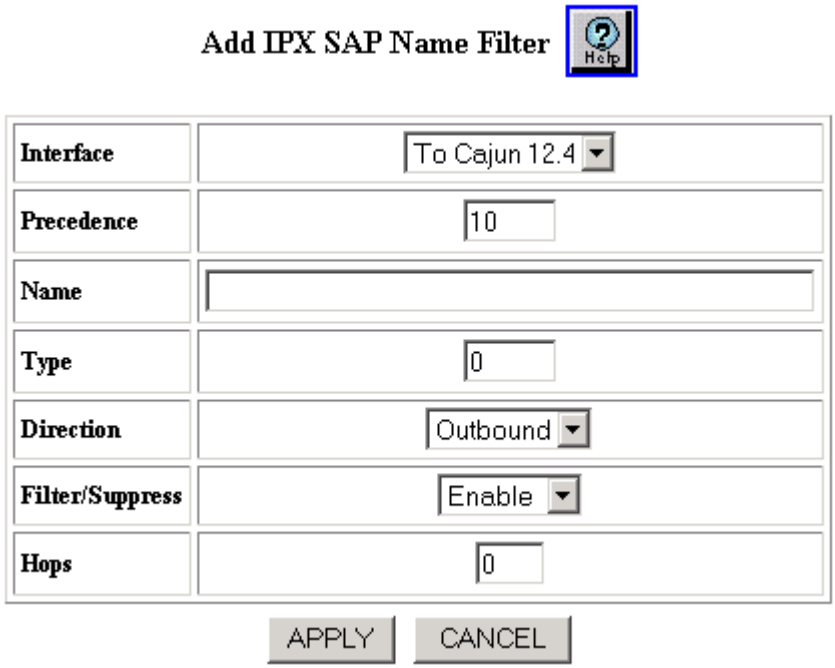
1. Select Name Filters from the **Routing > IPX > SAP** group on the Web Agent window. The IPX SAP Name Filters dialog box opens (Figure 6-113). Only the **CREATE** button is displayed when no **SAP filters** are configured.

***Figure 6-113. IPX SAP Name Filters Dialog Box.***




2. Select **CREATE** to create a new filter. The **Add IPX SAP Name Filter** dialog box opens (Figure 6-114).

*Figure 6-114. Add IPX SAP Name Filter Dialog Box*




3. Configure an IPX SAP name filter. Refer to Table 6-80 for an explanation of the **Add IPX SAP Name Filter** dialog box parameters:

*Table 6-80. IPX SAP Name Filter Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Interface** | Select the interface to which this filter will be applied to SAP packets sent and/or received on the interface from the pull-down menu. |
| **Precedence** | Enter the filter precedence (in order of importance) with 0 equal to most important.<br>**Note:** All SAP filters on the same interface must be assigned a unique precedence value. |
| **Name** | Enter a service name. For example, FS_ENG001. A single asterisk may be present as the last character, which will match all remaining characters of a service name. |

*Table 6-80. IPX SAP Name Filter Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Type** | Enter the service type that identifies the type of service the server provides.<br>Well-known service types include:<br>• Unknown (0)<br>• Print Queue (3)<br>• File Server (4)<br>• Job Server (5)<br>• Print Server (7)<br>• Archive Server (9)<br>• Remote Bridge Server (24)<br>• Advertising Print Server (47)<br>• NetWare Directory Services [NDS] (278)<br>A value of ffff matches all service type values. |
| **Direction** | Select the filter direction from the following pull-down menu options:<br>• **Inbound** - Applies the filter only to SAP packets received on the interface.<br>• **Outbound** - Applies the filter only to SAP packets sent on the interface (Default)<br>• **Both** - Applies the filter to SAP packets both sent and received on the interface. |
| **Filter/Suppress** | Select to enable or disable whether the services matching Name and Type are filtered (inbound) or suppressed (outbound).<br>• **Filtered** - Applies the filter only to SAP packets received (inbound direction) on the interface.<br>• **Suppressed** - Applies the filter only to SAP packets sent (outbound direction) on the interface.<br>Select **Enable** to filter/suppress traffic. Select **Disable** to disable the filtering and suppression of traffic.Default value is Enable. |
| **Hops** | Specify the number of routers (hops) that the packet must pass through before reaching the service(s) matched by the filter. This entry is used to override the value in the SAP packet.<br>Entering 0 ensures that there is no override in the transmission of data on the network. |

4. Click **APPLY to** save your changes, or **CANCEL** to restore previous settings.

**Example: Suppress Advertising of all Print Servers on Interface Remote**

To configure your switch to suppress the advertising of all Print Servers (for example, type 7) on Interface Remote:

1. Select **Name Filters** from the **Routing > IPX > SAP** group on the Web Agent window. The IPX SAP Name Filters dialog box opens (Figure 6-113).
2. Click **CREATE** to create a new filter. The **Add IPX SAP Name Filter** dialog box opens (Figure 6-114).
3. Configure the following parameters:
   a. Select **Remote** from the **Interface** pull-down menu.
   b. Enter 0 in the Precedence field.
   c. Enter * (asterisk) in the Name field. The asterisk represents a wildcard that applies to all server names.
   d. Enter 7 in the **Type** field.
   e. Select **Outbound** from the **Direction** pull-down menu.
   f. Select **Enable** from the **Filter/Suppress** pull-down menu.
   g. Enter 0 in the **Hops** field. This ensures that there is no override in the transmission of data on the network.
4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

*** Note:** This filter ensures that all advertising of any known print server on Interface Remote will be suppressed.

## Creating IPX SAP Name Filters Using the CLI

To create IPX SAP name filters using the CLI, enter the following command from Configure mode:

```
# ipx sap-name-filter <precedence> <filter-name>
<service-type> {outbound|inbound|both} {filter|
allow} [<filter-hops>]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for more details about this command.

# Creating IPX SAP Network Filters

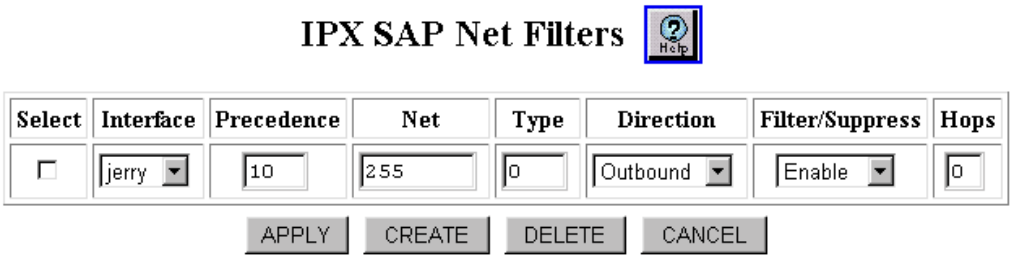
You can create IPX SAP network filters using wither the Web Agent or the CLI.

## Creating IPX SAP Network Filters Using the Web Agent

To create IPX SAP Network filters using the Web Agent:

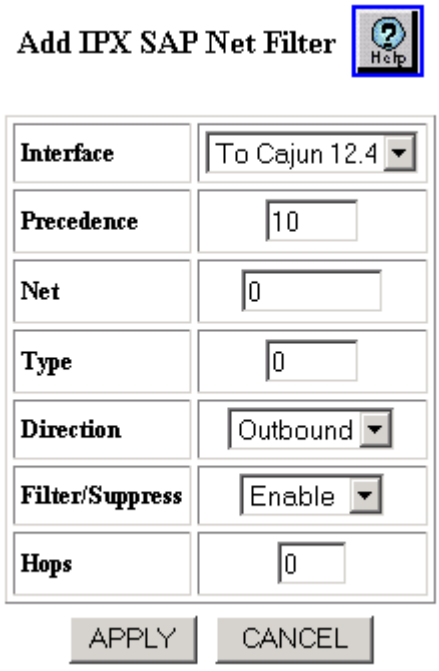
1. Select **Net Filters** from the **Routing > IPX > SAP** group on the Web Agent window. The **IPX SAP Net Filters** dialog box opens (Figure 6-115).Only the **CREATE** button is displayed when no IPX SAP Network Filers are configured.

***Figure 6-115. IPX SAP Net Filters Dialog Box***




2. Select **CREATE**. The **Add IPX SAP Net Filter** dialog box opens (Figure 6-116).

*Figure 6-116. Add IPX SAP Net Filter Dialog Box*




3. Refer to Table 6-81 to configure the **Add IPX SAP Net Filters** dialog box parameters:

*Table 6-81. Add IPX SAP Network Filter Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Select** | Select the IPX interface.<br>**Note:** This field is displayed in the **IPX SAP Net Filter** dialog box, not in the **Add IPX SAP Net Filter** dialog box. |
| **Interface** | Select the interface to which this filter will be applied to SAP packets sent and/or received on the interface. |
| **Precedence** | Specify the filter precedence (in order of importance) with 0 equal to most important.<br>**Note:** All SAP filters on the same interface must be assigned a unique filter precedence. |
| **Net** | Specify the network on which the server resides. A network number of ffffffff represents all networks. |

*Table 6-81. Add IPX SAP Network Filter Dialog Box Parameters*

| Parameter | Allows you to... |
|---|---|
| **Type** | Specify the service type (in hex) that identifies the type of service the server provides. Well-known service types include:<br>• Unknown (0)<br>• Print Queue (3)<br>• File Server (4)<br>• Job Server (5)<br>• Print Server (7)<br>• Archive Server (9)<br>• Remote Bridge Server (24)<br>• Advertising Print Server (47)<br>• NetWare Directory Services (278)<br>A value of ffff matches all service type values. |
| **Direction** | Select the direction of the filter in question. Filter choices include:<br>• **Inbound** - Applies the filter only to SAP packets received on the interface.<br>• **Outbound** - Applies the filter only to SAP packets sent on the interface.<br>• **Both** - Applies the filter to SAP packets both sent and received on the interface<br>Default value is outbound. |
| **Filter/ Suppress** | Disable whether the services matching Net and Type are filtered (inbound) or suppressed (outbound).<br>• **Filtered** - Applies the filter only to SAP packets received (inbound direction) on the interface.<br>• **Suppressed** - Applies the filter only to SAP packets sent (outbound direction) on the interface.<br>Select **Disable** to disable the filtering and suppression of traffic. The default is **Enable**. |
| **Hops** | Specify the number of routers (hops) that the packet must pass through before reaching the service(s) matched by the filter. This entry is used to override the value in the SAP packet.<br>Entering 0 ensures that there is no override in the transmission of data on the network. |

4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Example: Filtering all Services Except Netware Directory Services (NDS)

To configure your switch to filter all services except NDS a specific Interface, you must create two filters. Together, Filter 1 and Filter 2 filter services learned on the indicated interface except for NDS advertisements.

To create these filters using the Web Agent:

#### Filter 1

This filter ensures that all NDS packets received are not filtered on Interface Remote.

1. Select **Net Filters** from the **Routing > IPX > SAP** group on the Web Agent window. The **IPX SAP Net Filters** dialog box opens (Figure 6-115).
2. Select **CREATE**. The **Add IPX SAP Net Filter** dialog box opens (Figure 6-116).
3. Configure the following parameters:
   a. Select an interface name from the **Interface** pull-down menu.
   b. Enter 0 in the Precedence field.

      *** Note:** Any filter with a Precedence of 0 will always override a filter with a precedence of 1 or higher.

   c. Enter **ffffffff** (which represents all networks) in the **Net** field.
   d. Enter **278** (which represents the type for NDS) in the **Type** field.
   e. Select **Inbound** from the **Direction** pull-down menu.
   f. Select **Disable** from the **Filter/Suppress** pull-down menu to ensure that NDS advertisements are not filtered.
   g. Enter 0 in the **Hops** field to ensure that there is no override in the transmission of data on the network.

4. Click **APPLY** to save your changes, or CANCEL to restore previous settings.

**Filter 2**

Filter 2 ensures that all networks and service types are filtered for the indicated interface.

1. Select **Net Filters** from the **Routing > IPX > SAP** group on the Web Agent window. The IPX SAP Net Filters dialog box opens (Figure 6-115).
2. Click **CREATE** to create a new filter. The **Add IPX SAP Net Filter** dialog box opens (Figure 6-116).
3. Configure the following parameters:
   a. Select an interface name from the **Interface** pull-down menu.
   b. Enter 1 in the **Precedence** field.
   c. Enter **ffffffff** (which represents all networks) in the Net field.
   d. Enter **ffff** (which represents all services/types) in the Type field.
   e. Select **Inbound** from the **Direction** pull-down menu.
   f. Select **Enable** from the **Filter/Suppress** pull-down menu.
   g. Enter 0 in the **Hops** field. Entering 0 ensures that there is no override in the transmission of data on the network.
4. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Creating IPX SAP Network Filters Using the CLI

To create IPX SAP Network filters using the CLI, enter the following command from Interface mode:

```
(config if-<interface name>)# ipx
sap-network-filter <precedence> <filter-network>
<service-type> {outbound|inbound | both}
{filter|allow} [<filter-hops>]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# Interpreting IPX SAP Interface Statistics

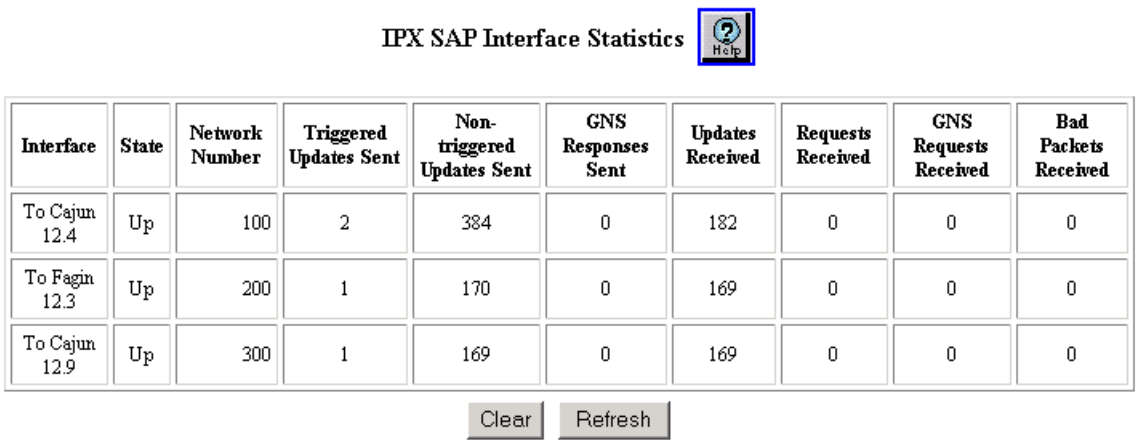
You can interpret IPX SAP interface statistics using either the Web Agent or the CLI.

## Interpreting IPX SAP Interface Statistics Using the Web Agent

To interpret IPX SAP interface statistic using the Web Agent:

1. Select Interface Statistics from the **Routing > IPX > SAP** group on the Web Agent window. The **IPX SAP Interface Statistics** dialog box opens (Figure 6-117).

*Figure 6-117. IPX SAP Interface Statistics Dialog Box*




2. Refer to Table 6-82 for an explanation of the **IPX SAP interface** statistics:

*Table 6-82. IPX SAP Interface Statistical Parameters*

| Parameter | Definition |
|---|---|
| Interface | The IPX interface associated with this SAP interface. |
| State | The current state of the SAP interface. |
| Network Number | The network number of the IPX network associated with the interface. |

***Table 6-82. IPX SAP Interface Statistical Parameters** continued*

| Parameter | Definition |
|---|---|
| Triggered Updates Sent | The number of triggered updates sent from the SAP interface. |
| Non-triggered Updates Sent | The number of non-triggered updates sent from the SAP interface. |
| GNS Responses Sent | The number of GNS responses sent from the SAP interface. |
| Updates Received | The number of updates received. Updates may be received periodically even if no changes have occurred. |
| Requests Received | The number of requests received on the SAP interface. |
| GNS Requests Received | The number of GNS requests received on the SAP interface. |
| Bad Packets Received | The number of bad packets received on the SAP interface. |

3. Click on **CLEAR** to remove the statistics, or **REFRESH** to access current interface statistics.

## Interpreting IPX SAP Interface Statistics Using the CLI

To interpret IPX SAP interface statistics using the CLI, enter the following command from Interface mode:

```
(config-if <interface name>)# show ipx interface
[<intf-name>]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# 15 Configuring AppleTalk Routing

## Overview

The following information and procedures provided in this chapter pertain to layer 3 module configuration only:

- Implementation
- Configuring AppleTalk Routing
- Viewing AppleTalk Statistics

## Implementation

This section introduces AppleTalk routing, explains how it operates, and explains why you would want to configure it on the Avaya P550R/P580/P880/P882 Multiservice switch.

### What is AppleTalk Routing?

AppleTalk Phase I was originally designed for local work groups. AppleTalk Phase II extends the number of nodes in an internetwork to over 16 million and the number of zones per port to 254. The Avaya switch supports both AppleTalk Phase I and Phase II. However, the translation from AppleTalk Phase I to Phase II is not supported.

*** Note:** The Avaya P550R/P580/P880/P882 Multiservice switch supports AppleTalk over Ethernet only.

The supported Ethernet versions are:

- Ethernet SNAP
- Ethernet II

The Avaya P550R/P580/P880/P882 Multiservice switch supports the following AppleTalk protocols:

- AppleTalk Address Resolution Protocol (AARP)

  This is an AppleTalk support protocol that maps the hardware address of an AppleTalk node to an Appletalk protocol address.

- Routing Table Maintenance Protocol (RTMP)

  This protocol maintains information about AppleTalk addresses and connections between different networks. Specially, it tells each router to:

  — Learn a new route to other routers

  — Delete a route if the local router has not broadcast that route to the network for a certain period of time.

- Name-Binding Protocol (NBP)

  This protocol translates alphanumeric entity names to AppleTalk addresses. NBP maintains a table of node addresses and entities within each node. Because each node also maintains it own list of named entities, the name directory within an AppleTalk network is not centralized. The names directory database is distributed among all nodes on the intranetwork.

- Datagram Delivery Protocol (DDP)

  This protocol transfers data in packets called datagrams.

- AppleTalk Echo Protocol (AEP)

  This protocol is used to send datagrams to other nodes in the network. The transmitted AEP datagram causes the destination node to return, or echo, that datagram to the sending node. This protocol determines whether a node is accessible before any sessions are started, and it enables users to estimate the round-trip delay time between nodes.

- Zone Information Protocol (ZIP)

  AppleTalk routers use this protocol to map network numbers to zones. Each AppleTalk router maintains a Zone information Table which lists the zone-to-network mapping information.

For more detailed information about these protocols, refer to the AppleTalk documentation.

## Need for AppleTalk Routing

If you configure your Avaya P550R/P580/P880/P882 Multiservice switch into a network running AppleTalk routing, you should be aware of the following:

- Appletalk is built into all Apple devices, thus making them automatically network capable. This makes Apple an extremely easy network system to install and maintain.
- Due to the naming mechanism that AppleTalk uses, users do not have to understand how AppleTalk works.
- AppleTalk supports a peer-to-peer network, thus dedicated servers or centralized network are not required.
- AppleTalk is plug-and-play (auto-configuring). Therefore, users can plug an Appletalk device into an AppleTalk network and use it immediately. No network configuration or assignments of network addresses are needed when you add a device to an AppleTalk network.
- AppleTalk support zones, which makes it easier for network administrators to define workgroups that consist of users and services that can span multiple networks segments.

# Configuring AppleTalk Routing

This section provides procedures for:

- Enabling AppleTalk Global Routing
- Creating an AppleTalk Routing Interface
- Editing AppleTalk Interfaces
- Deleting an AppleTalk Interface
- Creating an AppleTalk Static Route

- Editing AppleTalk Static Routes
- Deleting an AppleTalk Static Route
- Creating an AppleTalk Name-Binding Protocol (NBP) Filter
- Editing an AppleTalk NBP Filter
- Adding or Deleting Interfaces to an NBP Filter
- Creating an AppleTalk Zone Filter
- Editing an AppleTalk Zone Filter
- Adding or Deleting Interfaces to a Zone Filter

## Enabling AppleTalk Global Routing

To enable AppleTalk routing globally:

1. Select **Global Configuration** from the **Routing** > **AppleTalk** > **Configuration** group on the Web Agent window. The **AppleTalk Routing Global Configuration** dialog box opens (Figure 6-118).

*** Note:** AppleTalk Routing is disabled by default.

***Figure 6-118. AppleTalk Routing Global Configuration Window***

2. Select **Enable** from the **AppleTalk Routing** pull-down menu.
3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

# Creating an AppleTalk Routing Interface

You can create an AppleTalk routing interface using the Web Agent or CLI.

## Using the Web Agent

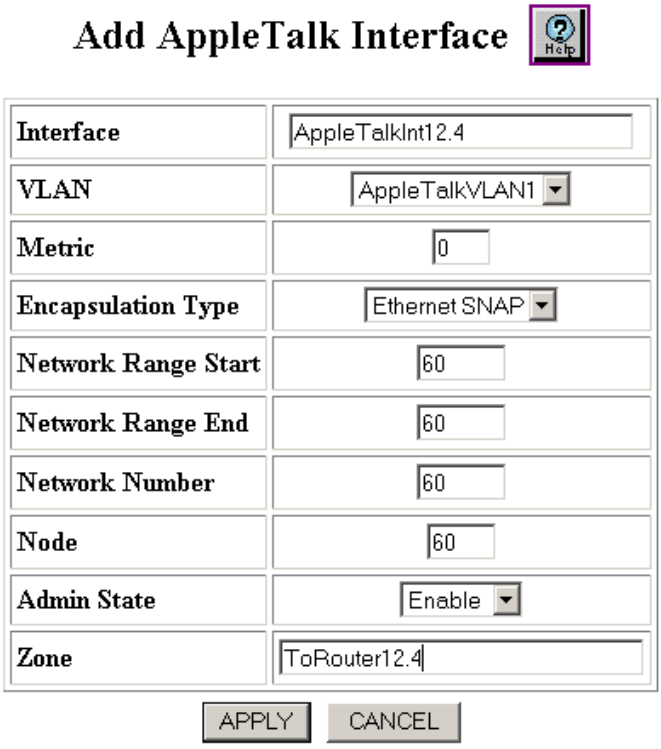
To create an AppleTalk routing interface using the Web Agent:

1. Enable AppleTalk routing globally. Refer to "Enabling AppleTalk Global Routing"", earlier in this chapter.
2. Select **Interfaces** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box opens (Figure 6-119).

***Figure 6-119. AppleTalk Interfaces Dialog Box***

3. Select **CREATE**. The **Add AppleTalk Interfaces** dialog box opens (Figure 6-120).

*Figure 6-120. Add AppleTalk Interfaces Dialog Box*




4. Refer to Table 6-83 to configure the **Add AppleTalk Interface** dialog box parameters:

*Table 6-83. Add AppleTalk Interface Dialog Box Parameters*

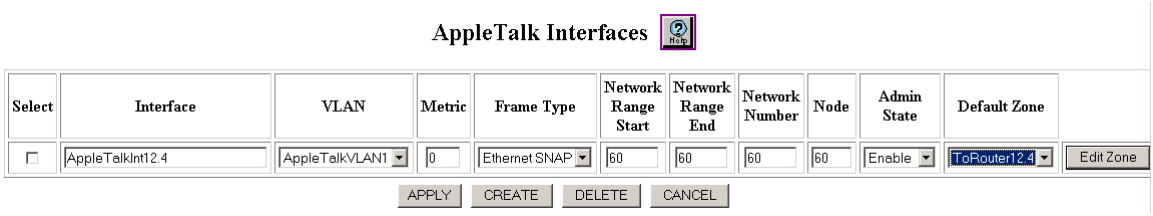
| Parameter | Definition |
|---|---|
| **Interface** | Enter the name of the AppleTalk interface to be created. 1 to 32 Characters |
| **VLAN** | Select the VLAN to be associated with the AppleTalk interface. |
| **Metric** | Enter the metric associated with the AppleTalk interface. |
| **Encapsulation Type** | Select the encapsulation type to be associated with the AppleTalk interface.The options include:<br>• **Ethernet II** - MTU = 1500<br>• **Ethernet SNAP** - MTU =1492 |

*Table 6-83. Add AppleTalk Interface Dialog Box Parameters*
*continued*

| Parameter | Definition |
|---|---|
| **Network Range Start** | Enter the starting network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 0 and 65279.<br>**Note:** The Network Range Start value must be less than or equal to the Network Range End value. |
| **Network Range End** | Enter the ending network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 0 and 65279.<br>**Note:** If the Network Range Start value equals 0, then the Network Range End value must also equal 0. |
| **Network Number** | Enter the interface network number. This number specifies the network number the interface is using.<br>**Note:** This value must be within the Network Range or be equal to 0. |
| **Node** | Enter the interface node identification number. This number must be between 1 and 253.<br>**Note:** Only if the Network Number is equal to 0, can the Node also be equal to 0. |
| **Admin State** | Select whether to enable or disable the administrator state. The administrator state determines if the interface is operational from a management point of view. |
| **Zone** | Select the default AppleTalk zone to be used by this interface. Zone names may be up to 32 characters in length. |

5. Click **Apply** to add the new AppleTalk interface, or **CANCEL** to restore previous settings. Once you click Apply, you are returned to the AppleTalk Interfaces dialog box (Figure 6-121.)

*Figure 6-121. AppleTalk Interfaces*




## Using the CLI

Use the following CLI commands in interface mode to create an AppleTalk interface:

```
(config if-:<interface-name>)# appletalk cable-range <cable-
range>
(config if-:<interface-name>)# appletalk address
<network.node>
(config if-:<interface-name>)# appletalk zone <zone-name>
(config if-:<interface-name>)# appletalk vlan <vlan-id>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Editing AppleTalk Interfaces

You can edit AppleTalk interfaces using either the Web Agent or the CLI.

## Using the Web Agent

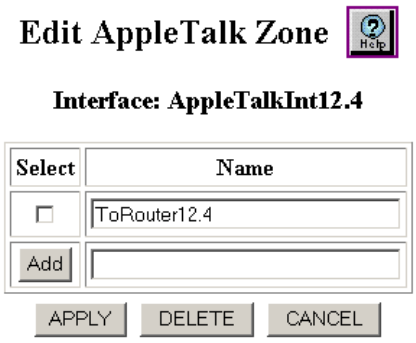
To edit an AppleTalk interface using the Web Agent:

*** Note:** You must enable AppleTalk globally and create an AppleTalk interface before you can edit an interface. See "Enabling AppleTalk Global Routing" and "Creating an AppleTalk Routing Interface", earlier in this section.

1. Select **Interfaces** from the R**outing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box opens (Figure 6-123).

2. If there is no zone to select or if you want to edit the zones available, complete this step through step x. If not, skip to step x+1. Select **Edit Zone** to edit the AppleTalk zone for this interface. The **Edit AppleTalk Zone** dialog box opens (Figure 6-122).

*Figure 6-122. Edit AppleTalk Zone Dialog Box*



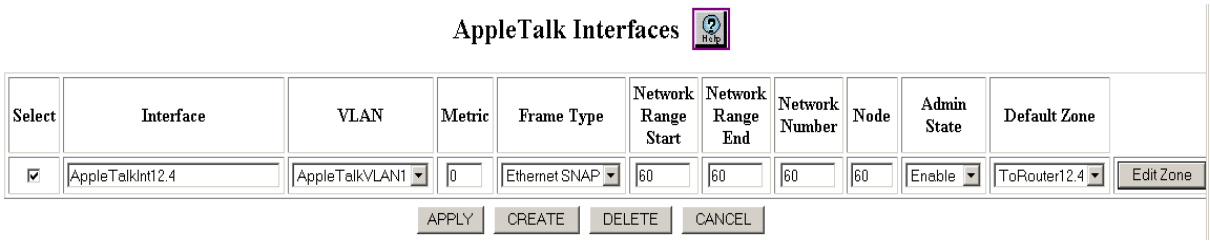

3. To add a new zone, enter the new AppleTalk zone name in the **Add text** field and click Add. Repeat this step as needed for each new zone on this interface.

4. To change a zone name(s), place a check mark(s) in the **Select** column and make the change(s) to the zone name(s). Click **Apply** to save the new AppleTalk zone, or either **Delete** or **Cancel** to remove the new zone.

5. Select **Interfaces** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box re-opens (Figure 6-123)

6. Select the new zone that you just created from the **Default Zone** field pull-down menu.

*Figure 6-123. AppleTalk Interfaces*




7. Make sure there is a check mark next to the interface(s) you will modify.

8. Select the VLAN to be associated with the interface from the **VLAN** field pull-down menu.

9. Enter the new port metric to be associated with the interface in the **Metric** field.

10. Select the new frame type to be associated with the interface from the **Frame Type** pull-down menu.

11. Enter the new network range start number in the N**etwork Range Start** field.

12. Enter the new network range end number in the **Network Range End** field.

13. Enter the new network number to be associated with the interface in the **Network Number** field.

14. Enter the new node number to be associated with the interface in the **Node** field.

15. Select **Enable** from the **Admin. State** field pull-down menu.

16. Select the new default zone associated with the interface from the **Default Zone** field pull-down menu.

17. Select the AppleTalk interface that you want to update in the **Select** column.

18. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

*** Note:** You may select and change multiple interfaces simultaneously with one APPLY operation.

### Using the CLI

To edit an AppleTalk interface using the CLI, enter the following command from Interface mode:

```
(config if-:<interface-name>)# appletalk <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Deleting an AppleTalk Interface

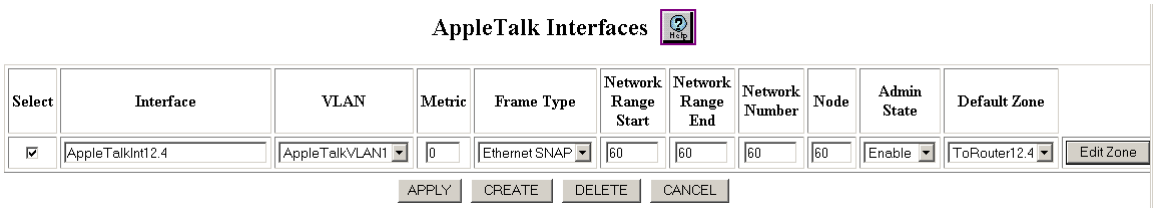
You can delete an AppleTalk interface using either the Web Agent or the CLI.

### Using the Web Agent

To delete an AppleTalk interface using the Web Agent:

1. Select **Interfaces** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box opens (Figure 6-124).

*Figure 6-124. AppleTalk Interfaces Dialog Box*




2. Select the AppleTalk interface that you want to delete from the **Select** column.

3. Click **DELETE** to remove the AppleTalk interface.

### Using the CLI

Use the following CLI commands in interface mode to delete an AppleTalk interface:

```
(config if-:<interface-name>)# no appletalk cable-range
<cable-range>
(config if-:<interface-name>)# no appletalk address
<network.node>
(config if-:<interface-name>)# no appletalk zone <zone-name>
(config if-:<interface-name>)# no appletalk vlan <vlan-id>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Creating an AppleTalk Static Route

You can create an AppleTalk static route using the Web Agent or the CLI.

### Using the Web Agent

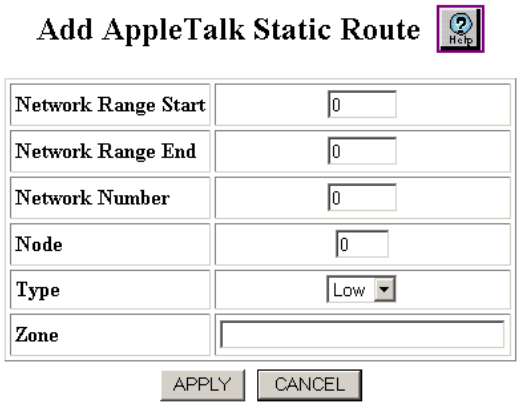
To create an AppleTalk static route using the Web Agent:

1. Select **Static Route** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Static Route** dialog box opens (Figure 6-125).

*Figure 6-125. AppleTalk Static Route Dialog Box*

2. Select **CREATE** to add a new static route. The A**dd AppleTalk Static Route** dialog box opens (Figure 6-126).

*Figure 6-126. Add AppleTalk Static Route Dialog Box*




3. Refer to Table 6-84 to configure the **Add AppleTalk Static Route** dialog box parameters.

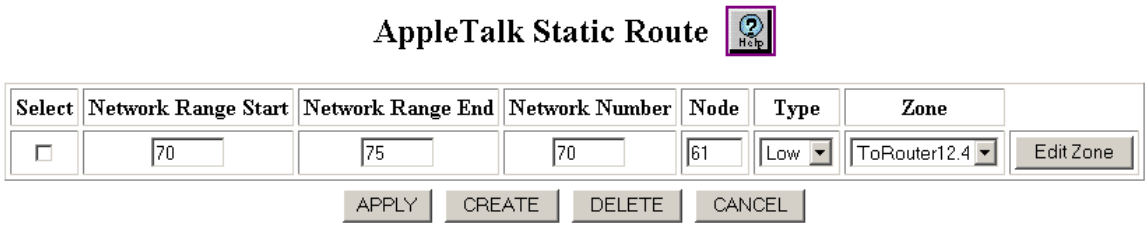
*Table 6-84. Add AppleTalk Static Route Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Network Range Start** | Enter the starting network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 1 and 65279.<br>**Note:** Network Range Start must be less than or equal to Network Range End. |
| **Network Range End** | Enter the ending network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 1 and 65279. |
| **Network Number** | Enter the next hop network number. This number specifies the network number of the next hop router for the network range. |

*Table 6-84. Add AppleTalk Static Route Dialog Box*

| Parameter | Definition |
|---|---|
| **Node** | Enter the next hop node identification number. This number must be between 1 and 253. |
| **Type** | Select the type of static route. The options include:<br>• **High** - The static route is not superseded by a route update.<br>• **Low** - The static route can be superseded by a route update. |
| **Zone** | Enter an AppleTalk zone name assigned to this route. Zone names may be up to 32 characters in length. |

4. Click **APPLY** to add the static route, or **CANCEL** to restore previous settings. When you click **APPLY**, you are returned to the AppleTalk Static Route dialog box.




### Using the CLI

To create an AppleTalk static route using the CLI, enter the following command in Interface mode:

```
(config if-<interface-name>:)# appletalk static
cable-range <cable-range> to <network.node>
[floating] zone <zone-name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Editing AppleTalk Static Routes

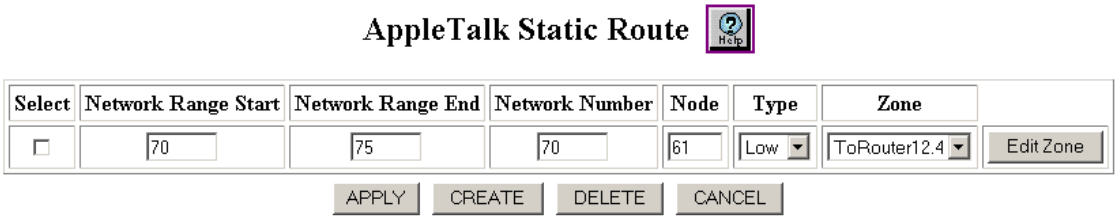
You can edit AppleTalk Static routes using either the Web Agent or the CLI.

### Using the Web Agent

To edit an AppleTalk static route using the Web Agent:

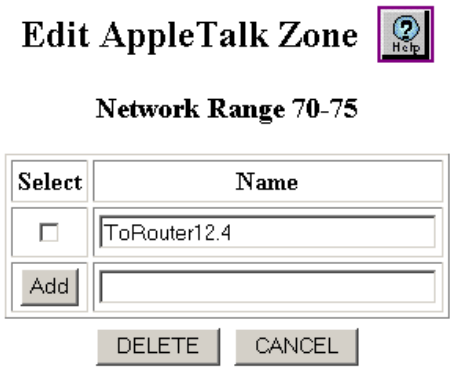
1. Select **Static Route** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Static Route** dialog box opens (Figure 6-125).

*Figure 6-127. AppleTalk Static Routes*




2. If you need to Add or Delete Zones, select **Edit Zone** otherwise, skip to step 4. The **Edit AppleTalk Zone** dialog box opens (see Figure 6-128)

*Figure 6-128. Edit AppleTalk Zone.*




3. If you need to add a new zone, enter the new AppleTalk zone name and click **Add** in the **Add text** field. If you need to delete a zone(s), place a check in the **Select** column next to the zone you need to delete then click the **DELETE** button.

4. Navigate back the AppleTalk Static Route dialog box by selecting **Static Route** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Static Route** dialog box opens (Figure 6-125).Select the AppleTalk Static Route that you want to edit from the **Select** column.

5. Enter the new network range start number in the **Network Range Start** field.

6. Enter the new network range end number in the **Network Range End** field.

7. Enter the new network number of the next hop for the static route in the **Network Number** field.

8. Enter the new node number of the next hop for the static route in the **Node** field.

9. Enter the type to be associated with the static route in the **Type** field.

10. Click **APPLY** to save the new zone.

### Using the CLI

To edit an AppleTalk static route using the CLI, enter the following command from Interface mode:

```
(config if-:<interface-name>)# appletalk static
cable-range <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Deleting an AppleTalk Static Route

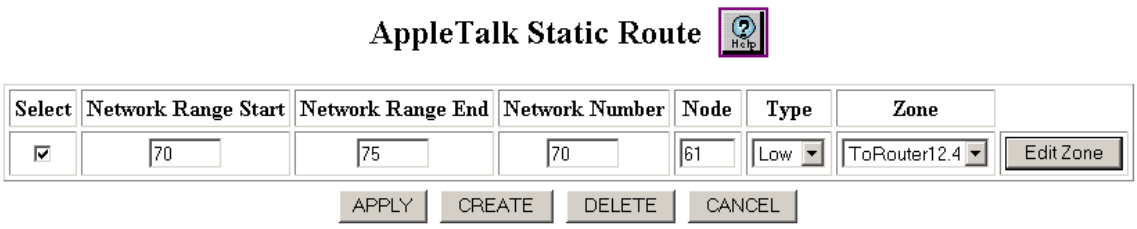
You can delete an AppleTalk static route using either the Web Agent or the CLI.

### Using the Web Agent

To delete an AppleTalk static route using the Web Agent:

1. Select **Static Route** from the R**outing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Interfaces** dialog box opens (Figure 6-129).

***Figure 6-129. AppleTalk Static Route***




2. Select the AppleTalk static route that you want to delete from the **Select** column.

3. Click **DELETE** to remove the AppleTalk static route.

### Using the CLI

To delete an AppleTalk static route using the CLI, enter the following command in **Configure** mode:

```
> (config if-<interface-name>:)# no appletalk
static
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Creating an AppleTalk Name-Binding Protocol (NBP) Filter

The NBP performs a conversion from named AppleTalk entities to their AppleTalk protocol addresses. Multiple names can exist for the same entity (alias). NBP also performs:

- Name registration
- Name deletion
- Name lookup
- Name confirmation

NBP allows you to bind a name to the internal storage address for your entity and register this mapping so that other entities can look it up. You can display NBP names to users and use addresses internally to locate entities. When you register your entity's name and address pair, NBP validates its uniqueness.

An NBP Filter prevents hosts on one or more interfaces from accessing hosts or services beyond that interface.

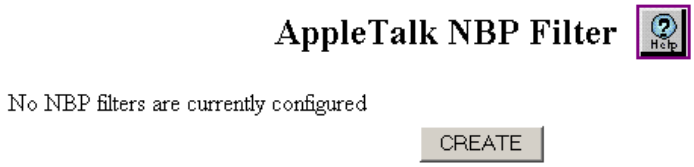
You can create an NBP Filter using either the Web Agent or the CLI.

## Using the Web Agent

To create an NBP Filter using the Web Agent:

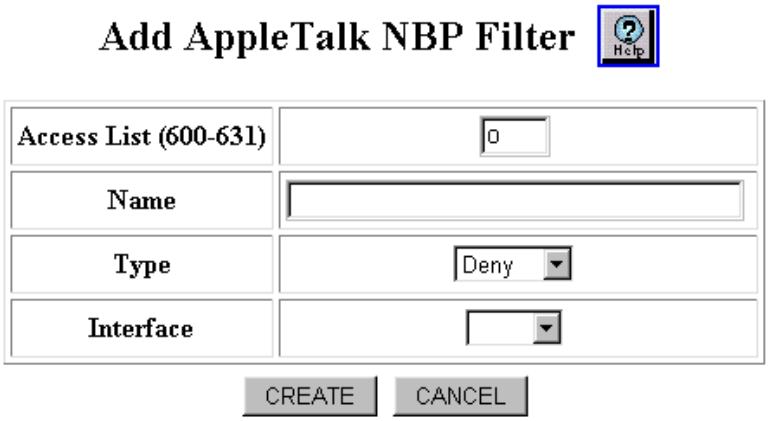
1. Select **NBP Filter** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk NBP Filter** dialog box opens (Figure 6-130).

***Figure 6-130. AppleTalk NBP Filter Dialog Box***




2. Select **CREATE** to add a new NBP filter. The **Add AppleTalk NBP Filter** dialog box opens (Figure 6-131).

*Figure 6-131. Add AppleTalk NBP Filter Dialog Box*




3. Refer to Table 6-85 to configure the **Add AppleTalk NBP filter** dialog box.

*Table 6-85. AppleTalk NBP Filter Parameters*

| Parameter | Definition |
|---|---|
| **Access List** | Enter the access list number to be associated with the NBP filter. Valid values are 600-631. |
| **Name** | Enter the name of the NBP name object to be filtered. |
| **Type** | Select the type of filtering. The options include:<br>• **Deny**<br>• Permit |
| **Interface** | Select the interface(s) to apply this filter to. |

4. Click **CREATE** to add your new static route, or **CANCEL** to restore previous settings.

## Using the CLI

To create an NBP filter using the CLI, enter the following command from Interface mode:

```
(config-if <interface-name>:)# appletalk access-
list <access-list-number> <permit | deny> nbp
<string>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Editing an AppleTalk NBP Filter

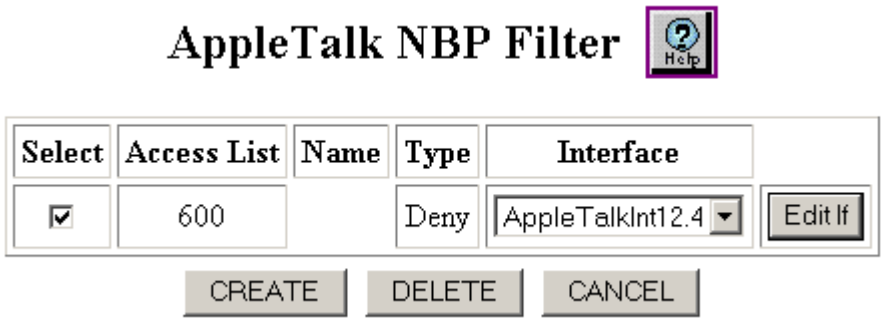
You can edit an AppleTalk NBP filter using either the Web Agent or the CLI.

## Using the Web Agent

To edit an AppleTalk NBP filter using the Web Agent:

1. Select **NBP Filter** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk NBP Filter** dialog box opens (Figure 6-132).

***Figure 6-132. AppleTalk NBP Filter***




2. Refer to Table 6-85 to edit the **AppleTalk NBP Filter** dialog box parameters.
3. Click:
   - **CREATE** to add a new filter. The **Add AppleTalk NBP Filter** dialog box opens. See "Creating an AppleTalk NBP Filter", earlier in this section, for more information.
   - **DELETE** to remove the selected NBP filter.
   - **CANCEL** to restore previous settings.
   - **Edit If** to add or delete this NBP filter to/from an interface. The **Add/Delete Interface to NBP Filter** dialog box opens. See "Adding or Deleting Interfaces to NBP Filter", later in this section, for more information.

## Using the CLI

To edit an AppleTalk NBP filter using the CLI, enter the following command in Interface mode:

```
(config-if <interface-name>:)# appletalk access-
list <access-list-number> <permit | deny> nbp
<string>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Adding or Deleting Interfaces to an NBP Filter

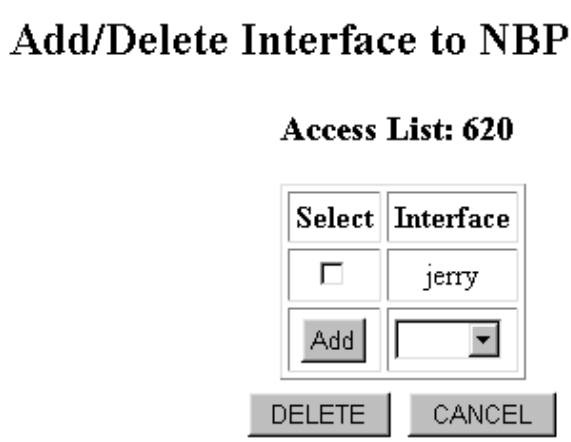
You can add or delete interfaces to an NBP filter using either the Web Agent or the CLI.

## Using the Web Agent

To add or delete interfaces to an NBP filter using the Web Agent:

1. Select **NBP Filter** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk NBP Filter** dialog box opens (see Figure 6-132).
2. Select **Edit If**. The **Add/Delete Interface to NBP Filter** dialog box opens (see Figure 6-133).

***Figure 6-133. Add/Delete Interface to NBP Filter Dialog Box***




3. Select the interface to be added from the **Add** field pull-down menu.

   Or

   Click an interface from the **Select** column for the interface that you want to be remove.

4. Click:
   - **Add** to add this NBP filter to the selected interface.
   - **DELETE** to remove this NBP filter from the selected interface.
   - **CANCEL** to restore previous settings.

### Using the CLI

To add interfaces to an NBP filter using the CLI, enter the following command from Interface mode:

```
(config-if <interface-name>:)# appletalk access-
list <access-list-number> <permit | deny> nbp
<string>
```

To delete interfaces to an NBP filter using the CLI, enter the following command from **Configure** mode:

```
> (config-if <interface-name>:)# no appletalk
access-list <access-list-number> <permit | deny>
nbp <string>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Creating an AppleTalk Zone Filter

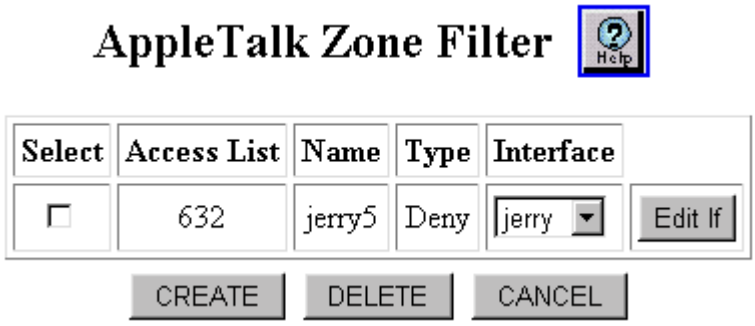
You can create an AppleTalk Zone Filter using either the Web Agent or the CLI.

### Using the Web Agent

To create an AppleTalk zone filter using the Web Agent:

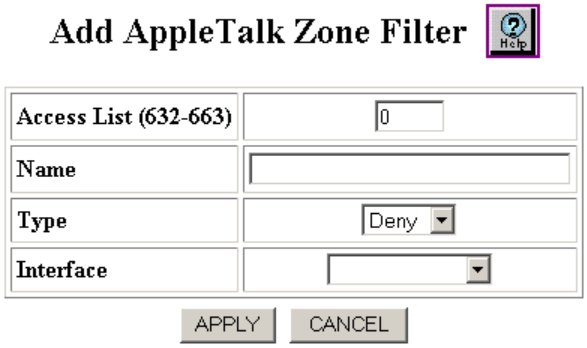
1. Select **Zone Filter** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Zone Filter** dialog box opens (Figure 6-134).

***Figure 6-134. AppleTalk Zone Filter Dialog Box***




2. Select **CREATE**. The **Add AppleTalk Zone Filter** dialog box opens (see Figure 6-135).

*Figure 6-135. Add AppleTalk Zone Filter Dialog Box*




3. Refer to Table 6-86 to configure the **Add AppleTalk Zone Filter** dialog box parameters:

*Table 6-86. Add AppleTalk Zone Filter Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Access List** | Enter the access list number to be associated with the zone filter. Valid values are 632-663. |
| **Name** | Enter the name of the zone to be filtered. You can also leave this field blank for wildcarding. |
| **Type** | Select the type of filtering. The options include:<br>• **Deny**<br>• **Permit** |
| **Interface** | Select the interface to apply this filter to. |

4. Click **APPLY** to add the new zone filter, or **CANCEL** to restore previous settings.

## Using the CLI

To create an AppleTalk zone filter using the CLI, enter the following command from Interface mode:

```
(config-if <interface-name>:)# appletalk access-
list <access-list-number> <permit | deny> zone
<string>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Editing an AppleTalk Zone Filter

You can edit an AppleTalk zone filter using either the Web Agent or the CLI.

## Using the Web Agent

To edit an AppleTalk zone filter using the Web Agent:

1. Select **Zone Filter** from the R**outing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Zone Filter** dialog box opens (Figure 6-135).
2. Click the checkbox in the **Select** column next to the AppleTalk zone filter that you want to be edit.
3. Refer to Table 6-86 to edit the **AppleTalk Zone Filter** dialog box parameters:.
4. Click:
   - **CREATE** to add a new zone filter. The **Add AppleTalk Zone Filter** dialog box opens. See "Creating an AppleTalk Zone Filter", earlier in this section for more information.
   - **DELETE** to remove the selected zone filter.
   - **CANCEL** to restore previous settings.
   - **Edit If** to add or delete this zone filter to/from an interface. The **Add/Delete Interface to Zone Filter** dialog box opens. See "Adding or Deleting Interfaces to a Zone Filter", later in this section for more information.

## Using the CLI

To edit an AppleTalk zone filter using the CLI, enter the following command from Interface mode:

```
(config-if <interface-name>:)# appletalk access-
list <access-list-number> <permit | deny> zone
<string>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Adding or Deleting Interfaces to a Zone Filter

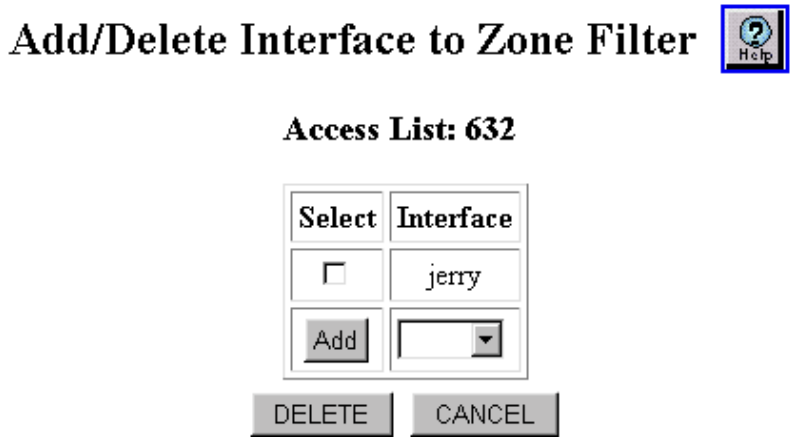
You can add or delete interfaces to a zone filter using either the Web Agent or the CLI.

## Using the Web Agent

To add or delete interfaces to a zone filter using the Web Agent:

1. Select **Zone Filter** from the **Routing > AppleTalk > Configuration** group on the Web Agent window. The **AppleTalk Zone Filter** dialog box opens (Figure 6-134).
2. Select **Edit** If. The **Add/Delete Interface to Zone Filter** dialog box opens (Figure 6-136).

*Figure 6-136. Add/Delete Interface to Zone Filter Dialog Box*




3. Select the interface to be added from the **Add** field pull-down menu.

   Or

   Click the checkbox in the **Select** column for the interface that you want to be remove.

4. Click:
   - **Add** to add this zone filter to the selected interface.
   - **DELETE** to remove this zone filter from the selected interface.
   - **CANCEL** to restore previous settings.

### Using the CLI

To add interfaces to a zone filter using the CLI, enter the following command from Interface mode:

```
(config-if <interface-name>:)# appletalk access-
list <access-list-number> <permit | deny> zone
<string>
```

To delete interfaces to an zone filter, enter the following command from Interface mode:

```
(config-if <interface-name>:)# no appletalk
access-list <access-list-number> <permit | deny>
zone <string>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Viewing AppleTalk Statistics

This section includes:


- Viewing AppleTalk Global Statistics
- Viewing the AppleTalk Interface Statistics Table
- Using the CLI
- Viewing AppleTalk Route Table Statistics
- Viewing the AppleTalk ARP Cache Table
- Viewing the AppleTalk Zone Table
- Viewing AppleTalk Zone Table Statistics
- Viewing the AppleTalk NBP Table


## Viewing AppleTalk Global Statistics

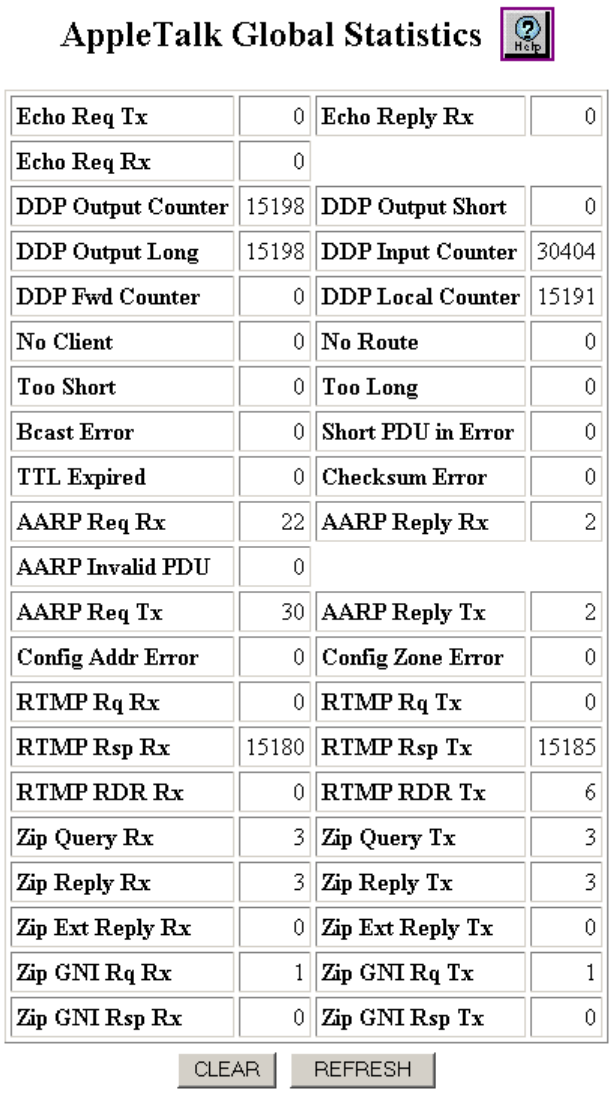
You can view AppleTalk global statistics using either the Web Agent or the CLI.

### Using the Web Agent

To view AppleTalk global statistics using the Web Agent:

1. Select **Global Statistics** from the R**outing > AppleTalk > Display** group on the Web Agent window. The A**ppleTalk Global Statistics** dialog box opens (Figure 6-137).

*Figure 6-137. AppleTalk Global Statistics Dialog Box*


AppleTalk Global Statistics
Help
Echo Req Tx 0 Echo Reply Rx 0
Echo Req Rx 0
DDP Output Counter 15198 DDP Output Short 0
DDP Output Long 15198 DDP Input Counter 30404
DDP Fwd Counter 0 DDP Local Counter 15191
No Client 0 No Route 0
Too Short 0 Too Long 0
Bcast Error 0 Short PDU in Error 0
TTL Expired 0 Checksum Error 0
AARP Req Rx 22 AARP Reply Rx 2
AARP Invalid PDU 0
AARP Req Tx 30 AARP Reply Tx 2
Config Addr Error 0 Config Zone Error 0
RTMP Rq Rx 0 RTMP Rq Tx 0
RTMP Rsp Rx 15180 RTMP Rsp Tx 15185
RTMP RDR Rx 0 RTMP RDR Tx 6
Zip Query Rx 3 Zip Query Tx 3
Zip Reply Rx 3 Zip Reply Tx 3
Zip Ext Reply Rx 0 Zip Ext Reply Tx 0
Zip GNI Rq Rx 1 Zip GNI Rq Tx 1
Zip GNI Rsp Rx 0 Zip GNI Rsp Tx 0
CLEAR
REFRESH

2. Refer to Table 6-87 for information about the **AppleTalk Global Statistics** dialog box parameters.

*Table 6-87. AppleTalk Global Statistical Dialog Box Parameters*

| Parameter | Number of... |
|---|---|
| **Echo Req Tx** | Echo requests transmitted. |
| **Echo Reply Rx** | Echo replies received. |
| **Echo Req Rx** | Echo requests received. |
| **DDP Output Counter** | DDP packets sent from this node. |
| **DDP Output Short** | DDP packets sent using the short format. |

*Table 6-87. AppleTalk Global Statistical Dialog Box Parameters continued*

| Parameter | Number of... |
|---|---|
| **DDP Output Long** | DDP packets sent using the long format. |
| **DDP Input Counter** | DDP packets received at this node. |
| **DDP Fwd Counter** | DDP packets forwarded through this node. |
| **DDP Local Counter** | DDP packets received destined for this node. |
| **No Client** | Packets received for which the destination socket was not known. |
| **No Route** | Packets received for which the destination route was not known. |
| **Too Short** | Packets received that were smaller than the minimum size allowed for an AppleTalk packet. |
| **Too Long** | Packets received that were larger than the minimum size allowed for an AppleTalk packet. |
| **Bcast Error** | Broadcast errors detected. |
| **Short PDU in Error** | Packets received that had a short PDU in error. |
| **TTL Expired** | Packets dropped because they timed out. |
| **Checksum Error** | Packets which had checksum in error. |
| **AARP Req Rx** | AppleTalk ARP requests received. |
| **AARP Reply Rx** | Appletalk ARP replies received. |
| **AARP Invalid PDU** | AppleTalk ARP requests received which were invalid. |
| **AARP Req Tx** | AppleTalk ARP requests transmitted. |
| **AARP Reply Tx** | AppleTalk ARP replies transmitted. |
| **Config Addr Error** | Configuration address errors detected. |
| **Config Zone Error** | Zone configuration errors detected. |
| **RTMP Rq Rx** | RTMP requests received. |
| **RTMP Rq Tx** | RTMP requests transmitted. |
| **RTMP Rsp Rx** | RTMP responses received. |
| **RTMP Rsp Tx** | RTMP responses transmitted. |
| **RTMP RDR Rx** | RTMP route data requests received. |
| **RTMP RDR Tx** | RTMP route data requests transmitted. |
| **Zip Query Rx** | ZIP queries received. |
| **Zip Query Tx** | ZIP queries transmitted. |
| **Zip Reply Rx** | ZIP replies received. |
| **Zip Reply Tx** | ZIP replies transmitted. |
| **Zip Ext Reply Rx** | ZIP extended replies received. |

*Table 6-87. AppleTalk Global Statistical Dialog Box Parameters continued*

| Parameter | Number of... |
|---|---|
| **Zip Ext Reply Tx** | ZIP extended replies transmitted. |
| **Zip GNI Rq Rx** | ZIP get net info request received. |
| **Zip GNI Rq Tx** | ZIP get net info request transmitted. |
| **Zip GNI Rsp Rx** | ZIP get net info response received. |
| **Zip GNI Rsp Tx** | ZIP get net info response transmitted. |

3. Click **REFRESH** to update all statistics, or **CLEAR** to reset all statistics to zero.

### Using the CLI

To view AppleTalk global statistics using the CLI, enter the following command from **Enable/Configure** mode:

```
# show appletalk traffic
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Viewing the AppleTalk Interface Statistics Table

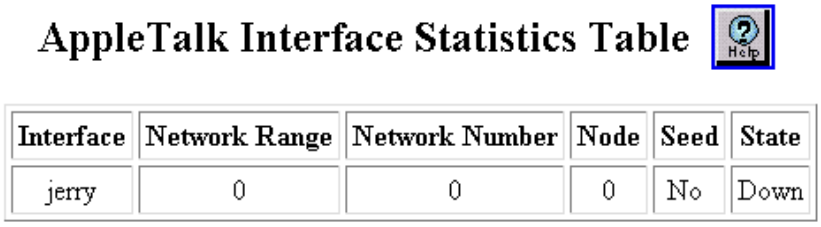
You can view the AppleTalk interface statistics table using either the Web Agent or the CLI.

### Using the Web Agent

To view the AppleTalk Interface statistics table using the Web Agent:

1. Select **Interface Statistics**.from the **Routing > AppleTalk > Display** group on the Web Agent window. The **AppleTalk Interface Statistics Table** opens (Figure 6-138).

*Figure 6-138. AppleTalk Interface Statistics Table*



AppleTalk Interface Statistics Table

| Interface | Network Range | Network Number | Node | Seed | State |
|---|---|---|---|---|---|
| jerry | 0 | 0 | 0 | No | Down |

2. Refer to Table 6-88 for information on the **AppleTalk Interface Statistics Table** parameters:

*Table 6-88. AppleTalk Interface Statistics Table Parameters*

| Parameter | Definition |
|---|---|
| **Interface** | Displays the name of the AppleTalk interface. |
| **Network Range** | Displays the network range associated with the AppleTalk interface. |
| **Network Number** | Displays the network number of this node. |
| **Node** | Displays the node number of this node. |
| **Seed** | Displays whether the AppleTalk interface seeded the network. |
| **State** | Displays the state of the AppleTalk interface. The options include:<br>• **Up** - indicates that the AppleTalk interface is active.<br>• **Down** - indicates that the AppleTalk interface is inactive. |

### Using the CLI

To view the AppleTalk Interface statistics table using the CLI, enter the following command from **Config** mode:

```
# show appletalk interface brief <CR> |
<interface-name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Viewing the AppleTalk Route Table

You can view the AppleTalk route table using the Web Agent or the CLI. You can also delete single entries from the table, or flush all of the routes from the table.

## Using the Web Agent

To view the AppleTalk route table, and delete or flush entries from the table using the Web Agent:

1. Select **Route Table** from the **Routing > AppleTalk > Display** group on the Web Agent window. The **AppleTalk Route Table** opens (Figure 6-139).

*Figure 6-139. AppleTalk Route Table Window*

2. Refer to Table 6-89 for information about the **AppleTalk Route Table** parameters:

*Table 6-89. AppleTalk Route Table Parameters*

| Parameter | Definition |
|---|---|
| **Select** | Select the entry to be acted upon. |
| **Network Range** | Displays the network range. |
| **Metric** | Displays the AppleTalk metric for the network range. |
| **State** | Displays the state of the entry.The options include:<br>• Good<br>• Suspect<br>• Going Bad<br>• Bad |
| **Owner** | Displays the AppleTalk component responsible for the addition of the route.The options include:<br>• Local<br>• Static<br>• RTMP |
| **Next Hop** | Displays the next hop address where forwarded packets are routed. |

*Table 6-89. AppleTalk Route Table Parameters continued*

| Parameter | Definition |
|---|---|
| **Interface** | Displays the Appletalk interface associated with the route table entry. |
| **Zones** | Displays the zones associated with the selected AppleTalk route. |

3. Click **Delete Entries** to remove selected route table entries.

   Or

   Click **Flush Route Table** to empty the route table of all dynamic entries. Static and Local entries are not flushed.

### Using the CLI

To view the AppleTalk Interface statistics table using the CLI, enter the following command:

```
># show appletalk route
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Viewing AppleTalk Route Table Statistics

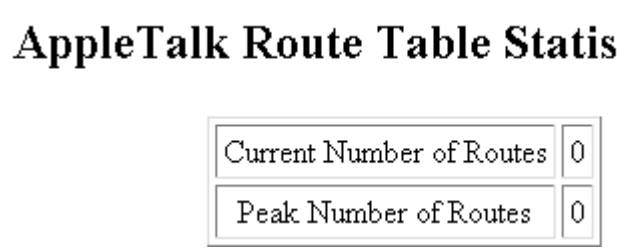
You can view AppleTalk route table statistics using either the Web Agent or the CLI.

### Using the Web Agent

To view AppleTalk route table statistics using the Web Agent:

1. Select **Route Table Statistics** from the **Routing > AppleTalk > Display** group on the Web Agent window. The **AppleTalk Route Table Statistics** dialog box opens (Figure 6-140).

*Figure 6-140. AppleTalk Route Table Statistics Dialog Box*



2. Refer to Table 6-90 for information on **AppleTalk Route Table Statistics** dialog box parameters:

*Table 6-90. AppleTalk Route Table Statistics Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Current Number of Routes** | Displays the current number of AppleTalk routes. |
| **Peak Number of Routes** | Displays the peak number of AppleTalk routes. |

### Using the CLI

Currently there is no CLI command to show appleTalk Route Statistics.

## Viewing the AppleTalk ARP Cache Table

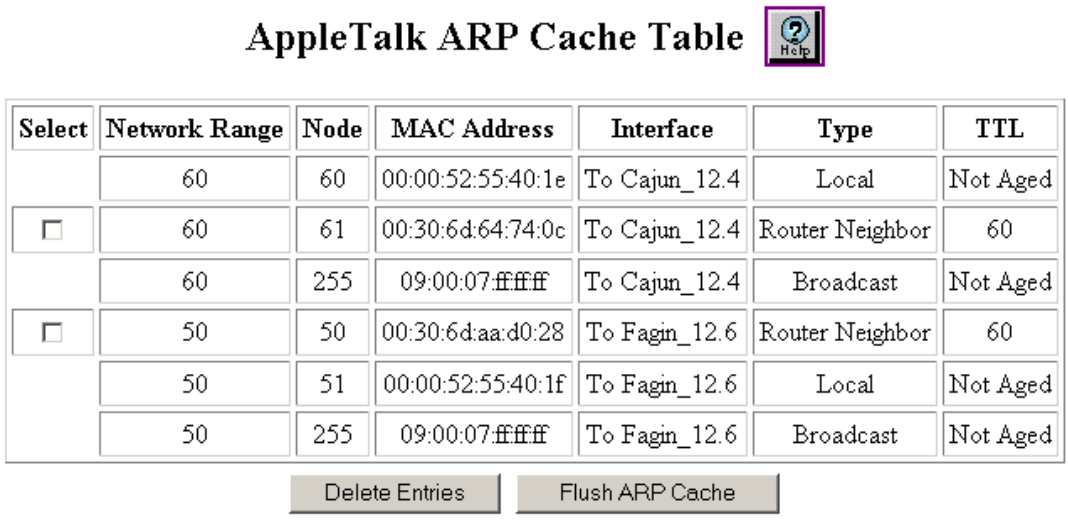
You can view the AppleTalk ARP cache table using either the Web Agent or the CLI.

### Using the Web Agent

To view the AppleTalk ARP cache table using the Web Agent:

1. Select **ARP Table** from the **Routing > AppleTalk > Display** group on the Web Agent window. The **AppleTalk ARP Cache Table** opens (see Figure 6-141).

*Figure 6-141. AppleTalk ARP Cache Table*



2. Refer to Table 6-91 for a definition of the **AppleTalk ARP Cache Table** parameters.

*Table 6-91. AppleTalk ARP Cache Table Parameters*

| Parameter | Definition |
|---|---|
| **Select** | Select the table entry to be acted upon. |
| **Network Range** | Displays the network range. |
| **Node** | Displays the node number for the entry. |
| **MAC Address** | Displays the MAC address associated with the AppleTalk ARP cache table entry of the node. |
| **Interface** | Displays the AppleTalk interface associated with the AppleTalk ARP cache table entry. |
| **Type** | Displays the type of cache entries.The values are:<br>• Local<br>• Broadcast<br>• Dynamic<br>• Router Neighbor |
| **TTL** | Displays the time-to-live value for the selected AppleTalk ARP cache table entry. Local and Broadcast entries do not time out. |

3. Select the checkbox next to any specific ARP entries that you want to delete and click **Delete Entries**.

   or

   Click **Flush Route Table** to reset the ARP cache table entries. Only Dynamic and Router Neighbor entries are flushed.

### Using the CLI

To view the AppleTalk ARP cache table using the CLI, enter the following command from **User** mode:

```
>show appletalk arp [all]
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Viewing the AppleTalk Zone Table

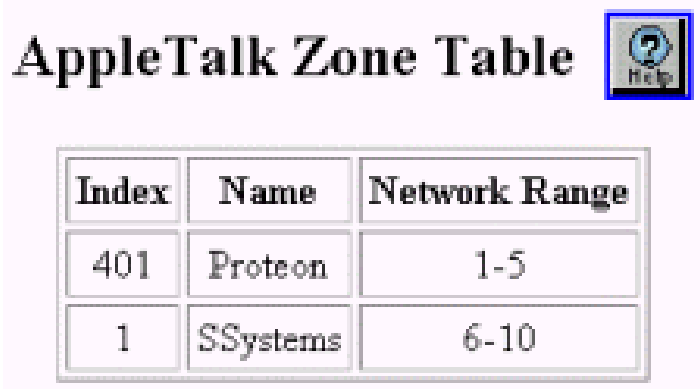
You can view the AppleTalk Zone table using either the Web Agent or the CLI.

### Using the Web Agent

To view the AppleTalk zone table using the Web Agent:

1. Select **Zone Table** from the **Routing > AppleTalk > Display** group on the Web Agent window. The **AppleTalk Zone Table** opens (Figure 6-142).

*Figure 6-142. AppleTalk Zone Table*




2. Refer to Table 6-92 for an explanation of the **AppleTalk Zone Table** parameters.

*Table 6-92. AppleTalk Zone Table Parameters*

| Parameter | Definition |
|---|---|
| **Index** | Displays the zone index. |
| **Name** | Displays the zone name. |
| **Network Range** | Displays the network range associated with the zone. |

### Using the CLI

The command to show AppleTalk Zone Statistics currently does not exist.

## Viewing AppleTalk Zone Table Statistics

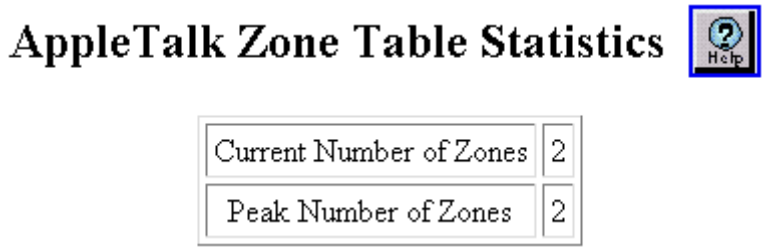
You can view the AppleTalk Zone Table Statistics using either the Web Agent or the CLI.

### Using the Web Agent

To view AppleTalk zone table statistics using the Web Agent:

1. Select **Zone Table Statistics** from the **Routing > AppleTalk > Display** group on the Web Agent window. The **AppleTalk Zone Table Statistics** table opens (Figure 6-143).

***Figure 6-143. AppleTalk Zone Table Statistics Table***




2. Refer to Table 6-93 for an explanation of the **AppleTalk Zone Table Statistics** parameters.

***Table 6-93. AppleTalk Zone Table Statistical Parameters***

| Parameter | Definition |
|---|---|
| **Current Number of Zones** | Displays the current number of AppleTalk zones. |
| **Peak Number of Zones** | Displays the peak number of AppleTalk zones. |

### Using the CLI

To view AppleTalk zone table statistics using the CLI, enter the following command from **User** mode:

```
> # show appletalk zone <cr | zone-name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Viewing the AppleTalk NBP Table

You can view the AppleTalk NBP Table using either the Web Agent or the CLI.

### Using the Web Agent

To view the AppleTalk NBP table using the Web Agent:

1. Select **Zone Table** from the **Routing > AppleTalk > Display** group on the Web Agent window. The **AppleTalk Zone Table** opens (Figure 6-142).

2. Refer to Table 6-94 for an explanation of the AppleTalk NBP Table parameters:

***Table 6-94. AppleTalk NBP Table Statistical Parameters***

| Parameter | Definition |
|---|---|
| **Index** | Displays the index of the name binding protocol entry. |
| **Name** | Displays the name of the NBP entry. |
| **Type** | Displays the type of object named. |
| **Interface** | Displays the AppleTalk interface associated with the AppleTalk NBP table entry. |
| **Zone** | Displays the zone field associated with the NBP table entry. |

## Using the CLI

To view the AppleTalk NBP table using the CLI, enter the following command from **User** mode:

```
> show appletalk nbp <cr | nbp-name>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# 16 Managing Intelligent Multicasting

## Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:


- Introduction
- Configuring Global Intelligent Multicasting
- Displaying Router Ports
- Configuring Static Router Ports
- Searching for Intelligent Multicast Sessions
- Creating a Static Multicast Session
- Managing Internet Group Management Protocol (IGMP) Snooping
- Managing the Lucent Group Management Protocol (LGMP) Server
- Managing the Lucent Group Management Protocol (LGMP) Client
- Managing Cisco Group Management Protocol (CGMP) Snooping


## Introduction

Intelligent multicasting refers to the forwarding of multicast traffic (packets with a multicast destination MAC address) within a VLAN to a subset of ports participating in that VLAN. It limits the forwarding of multicast traffic to only those ports on the VLAN with clients that want to receive this multicast traffic.

When disabled, intelligent multicasting floods layer 2 multicast traffic to all ports on the VLAN on which the traffic is received.

All traffic that is sent to a particular multicast MAC address is said to be in a multicast session. The switch supports 58 sessions per VLAN. Each multicast session keeps track of which ports must receive that session's multicast traffic within the VLAN. There are two types of ports: client ports and router ports.

A client port is a port with an attached host configured to receive a multicast session.

Router ports are ports that are attached to (or in the path to) multicast routers and must be treated specially. All multicast traffic on a VLAN must be forwarded to the router port.

Configuration of an Intelligent Multicast session first requires a session to be established. Once that session is established, client and router ports can be added to or removed from the session. Session and port configuration can be done either manually or dynamically. Dynamic intelligent multicasting is achieved through Internet Group Management Protocol (IGMP) Snooping, and may also involve Lucent Group Membership Protocol (LGMP), or Cisco Group Management Protocol (CGMP) Snooping. All of the dynamic mechanisms are based on the assumption that the client host is running IGMP, and is requesting membership in the IP multicast session.

*** Note:** If there is no multicast session created for a multicast flow in a VLAN, then that multicast flow will be flooded to all ports on the VLAN. This is the default behavior for a bridge as described in IEEE 802.1D. Intelligent multicasting must be enabled for any dynamic intelligent multicasting to be active.

By default, the switch rate limits inter-router multicast traffic on all modules that support rate limiting. If you need for your switch to support heavy multicast traffic, disable rate limiting on ports that are connected to routers. Also note that if high-bandwidth multicast streams are being used, rate limiting will affect directly connected clients if that stream is not part of an Intelligent Multicast session.

## Manually Configured Intelligent Multicasting

Manual configuration of Intelligent Multicast sessions allows the network administrator to dictate which multicast streams will be intelligently multicasted. This method of configuration is also useful where dynamic Intelligent Multicasting can not be used. Dynamic Intelligent Multicasting can only be used in an environment that uses IGMP and an IP multicast routing protocol (optional) to distribute multicast streams.

# Dynamic Intelligent Multicasting

In an environment that uses IGMP (and an IP multicast routing protocol, optionally), Dynamic Intelligent Multicasting may be used. The ability of the switch to dynamically set up sessions and add or remove client and router ports is particularly useful in a flexible multicast environment where there are many multicast sessions to administer. The protocols and mechanisms used to perform Intelligent Multicasting are enabled or disabled across all VLANs on a switch. The Dynamic Intelligent Multicasting process is split into three parts: Learning, Administration, and Dissemination.

## The Learning Process, IGMP Snooping

To learn which sessions must be configured, or which client or router ports must be added or removed, a mechanism to draw that information from the layer 3 protocols must be enabled. For the Avaya Multiservice Switch, IGMP Snooping is that mechanism. IGMP Snooping can learn about multicast sessions from IP interfaces that reside on the same switch.

*** Note:** IGMP Snooping is only available for VLANs that have an IGMP interface enabled.

Enabling DVMRP on an interface also enables IGMP.

## The Administration Process; Management and Pruning

At the core of all Intelligent Multicast functionality, the Administration Process is manipulated by manual configuration and dynamic configuration, and implements a pruning function. In a dynamically configured environment, the Administration Process takes the information from the Learning Process (from IGMP Snooping) or from one of the clients in the Dissemination Process and creates the AFT table entries which will perform the actual Intelligent Multicast functionality on the local switch. It also passes the new information to the servers in the Dissemination Process for distribution to other switches in the same VLAN.

The Administration Process views all data inputs as **applications.** Manual configuration is the MGMT (management) application, IGMP Snooping is the IGMP application, the LGMP client is the LGMP application, and the CGMP snooper is the CGMP application.

The pruning functionality of the Administration Process is a cleanup facility that prevents stale information from existing in the Intelligent Multicast tables in the event an application fails to perform its own cleanup. There are three types of pruning, each with their own timers: session, client port, and router port.

Automatic Session Pruning, if enabled, will remove a session if that session has not been active for Session Pruning Time.

Automatic Client Port Pruning, if enabled, will remove a client port from a session if no IGMP reports have been received on that port for that session in the time specified.

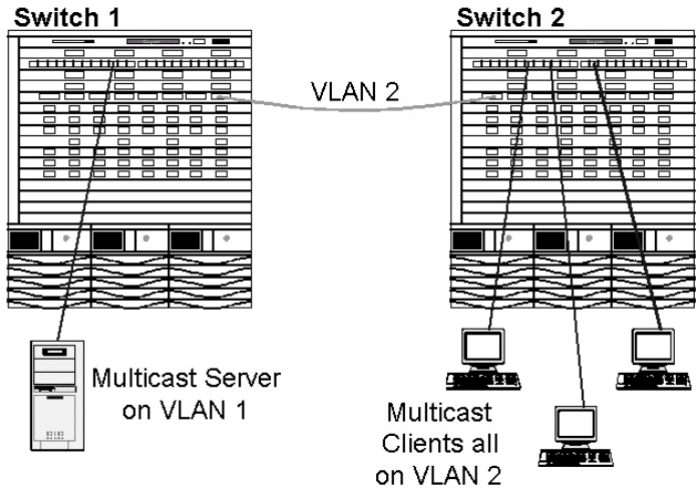
*** Note:** By enabling Automatic Client Port Pruning, there is a chance that the switch may disrupt multicast service temporarily to clients requesting to receive that multicast traffic. This is because of the report suppression mechanism in IGMP v1 and v2.

Automatic Router Port pruning, if enabled, will prune quiet router ports. If the switch has not been notified that there is a router on the port in Router Pruning Time, then the router port is removed.

## The Dissemination Process, LGMP and CGMP Snooping

The Dissemination Process provides a method to dynamically configure multicast sessions on switches with VLANs that do not have IP interfaces. See Figure 16-1

***Figure 6-144. LGMP and CGMP Snooping***




Switch 1 will route the multicast traffic from the Multicast Server on VLAN 1 to VLAN 2. Switch 2 does not have an IP interface on VLAN 2. Because the Learning Process requires an IP interface to perform learning, a different method must be used to create multicast sessions on Switch 2. Switch 1 must disseminate the Intelligent Multicast information to all switches on the attached VLANs that do not have IP interfaces. Two protocols are available for this use on the Switch, LGMP and CGMP.

LGMP and CGMP are similar protocols. Both protocols have a server implementation that runs on a switch that implements the Learning Process, and both protocols have a client implementation which runs on switches that do not have local IP interfaces on all involved VLANs. For the Avaya Multiservice switch, only the client implementation of CGMP is available in case the switch is connected to a Cisco router. This implementation is called CGMP Snooping.

*** Note:** IGMP Snooping must be enabled to learn the sessions that the LGMP server will disseminate. An LGMP server is active only for VLANs that have an IGMP interface enabled.

# Configuring Intelligent Multicasting

This section provides the following procedures:

- Configuring Global Intelligent Multicasting
- Displaying Router Ports
- Configuring Static Router Ports
- Searching for Intelligent Multicast Sessions
- Deleting an Intelligent Multicast Session
- Deleting a Multicast Session Client Port
- Creating a Static Multicast Session
- Deleting Static Multicast Sessions
- Creating Static Client Ports
- Deleting Static Client Ports

## Configuring Global Intelligent Multicasting

You can configure intelligent multicasting globally using either the Web Agent or the CLI.

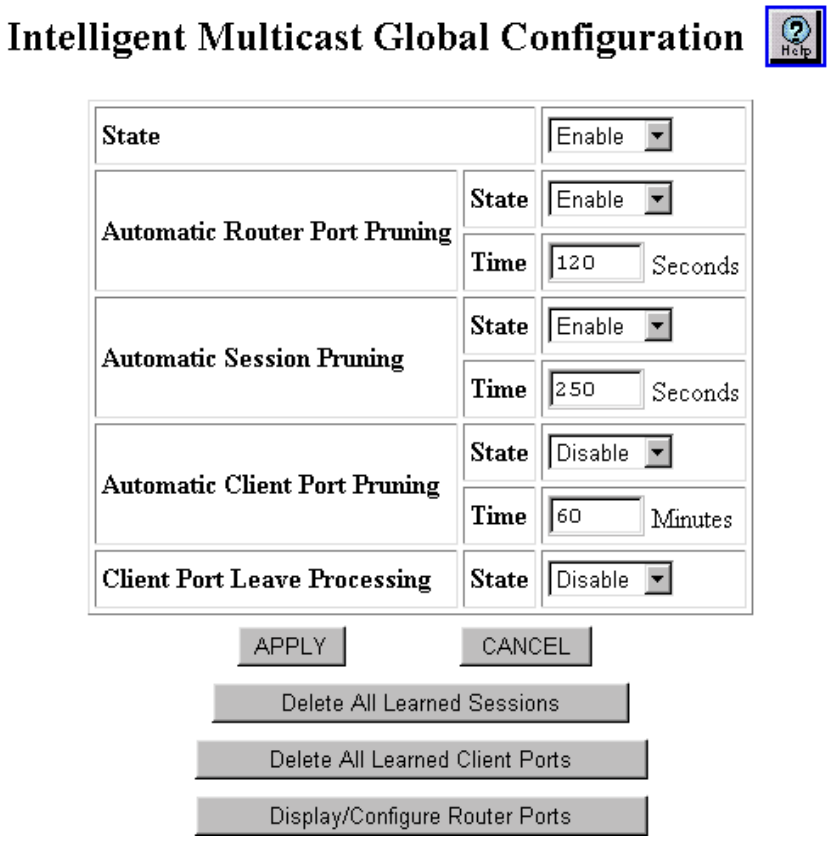
### Using the Web Agent

To configure intelligent multicasting globally using the Web Agent:

1. Select Global Configuration from the Layer 2 Switching > Intelligent Multicast group on the Web Agent window. The Intelligent Multicast Global Configuration dialog box opens (Figure 16-2).

*** Note:** You cannot delete Static sessions and client ports from this dialog box. Refer to "Deleting a Multicast Session Client Port" and "Deleting Static Multicast Sessions", in this chapter to delete static sessions and client ports.

***Figure 6-145. Intelligent Multicasting Global Configuration Dialog Box***




*** Note:** In order to route multicast traffic, IP multicast forwarding must be enabled on the switch. Refer to "Enabling IP Forwarding (Routing) Global Parameters", in Chapter 9, Configuring IP Routing.

2. Refer to Table 6-95 to configure the Intelligent Global Multicast Configuration dialog box parameters:

***Table 6-95. Intelligent Global Multicast Configuration Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Enable State** | Select **Disable** to prevent intelligent multicasting globally. The default value is **Enabled**. |
| **Automatic Router Port Pruning** | Select:<br>• **Disable** - to prevent automatic router port pruning. The default value is **Enable**.<br>• **Time** - Enter the time, in seconds, after which quiet learned router ports can be pruned. The valid range (in seconds) is 10 to 172800 (48 hours). The default value is **120 seconds**. |
| **Automatic Session Pruning** | Select:<br>• **Disable** - To prevent automatic removal of stale sessions. The default value is **Enable**.<br>• **Time** - Enter the time, in seconds, after which stale learned sessions can be removed. The valid range (in seconds) is 10 to 172800 (48 hours). The default value is **250 seconds**. |
| **Automatic Client Port Pruning** | Select:<br>• **Disable** - to prevent the automatic removal of quiet learned client ports from a session. The default value is **Disable**.<br>• **Time** - Enter the time, in minutes, after which quiet learned client ports can be automatically removed from a session. The valid range (in minutes) is 1 to 1440 (24 hours). The default value is **60 minutes**. |

3. Click

— **APPLY** to save your changes.

— **CANCEL** to restore previous settings.

— **Delete All Learned Sessions** to remove all learned multicast sessions.

— **Delete All Learned Client Ports** to remove all learned client ports from all multicast sessions.

— **Display/Configure Router Ports** to display the router ports and configure your static router ports.

### Using the CLI

To configure intelligent multicasting globally using the CLI, enter the following command from **Configure** mode:

```
<configure># set intelligent-multicast {enable}
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Displaying Router Ports

You can display router ports using either the Web Agent or the CLI.

### Using the Web Agent

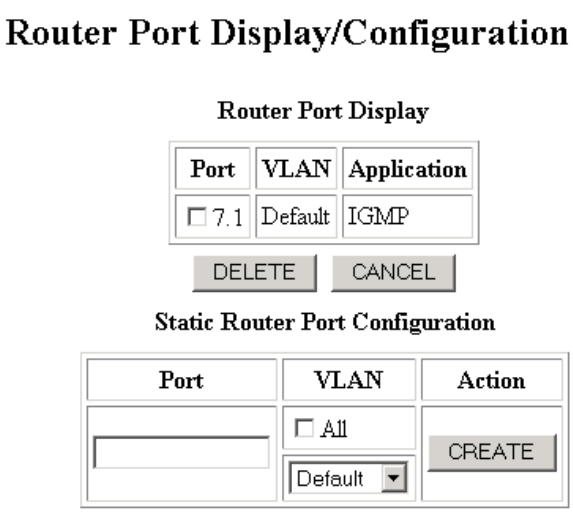
To display router ports using the Web Agent:

1. Select **Global Configuration** from the **L2 Switching > Intelligent Multicast** group on the Web Agent window. The **Intelligent Multicast Global Configuration** dialog box opens (Figure 16-2).

   *** Note:** You must enable intelligent multicasting on a global basis to make your router ports active. See "Configuring Global Intelligent Multicasting", earlier in this chapter.

2. Select **Display/Configure Router Ports**. The **Router Port Display/Configuration** dialog box opens (Figure 16-3).

***Figure 6-146. Router Port Display/Configuration Dialog Box***



3. Refer to Table 6-96 for an explanation of the **Router Port Display/Configuration** Dialog Box parameters.

***Table 6-96. Router Port Display/Configuration Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Port** | Displays the switch port configured as a router port. |
| **VLAN** | Displays which VLAN the router port is bound to. |
| **Application** | Displays the active applications of the router port. The applications include:<br>• Mgmt (Static)<br>• IGMP<br>• LGMP<br>• CGMP |

4. Select a router port from the **Port** column and click **DELETE** to delete the port, or **CANCEL** to restore previous settings.

### Using the CLI

To display router ports using the CLI, enter the following command from User mode:

```
# show intelligent-multicast router-port
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Configuring Static Router Ports

You can configure Static Router ports using either the Web Agent or the CLI.

### Using the Web Agent

To configure a static router port using the Web Agent:

1. Select **Global Configuration** from the **L2 Switching > Intelligent Multicast** group on the Web Agent window. The **Intelligent Multicast Global Configuration** dialog box opens (Figure 6-145).

*** Note:** You must enable intelligent multicasting on a global basis to make your static router port configuration active. See "Configuring Global Intelligent Multicasting", earlier in this chapter.

2. Select **Display/Configure Router Ports**. The **Router Port Display/Configuration** dialog box opens (Figure 16-3).
3. Enter a port number in the **Port** field.
4. Select **All** from the **VLAN** column to add this router port to all VLANs

   Or

   Select a specific VLAN from the VLAN field pull-down menu.

   *** Note:** When adding a router port to all VLANs, the router port is added only to the VLANs bound to the switch port. To bind multiple VLANs to a switch port, refer to "Using VLANs, Spanning Tree, Hunt Groups, and VTP Snooping" in Chapter 4.

5. Click **CREATE** to save your changes.

### Using the CLI

To configure a static router port using the CLI, enter the following command from Configure mode:

```
<configure># set intelligent-multicast router-port
vlan <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Searching for Intelligent Multicast Sessions

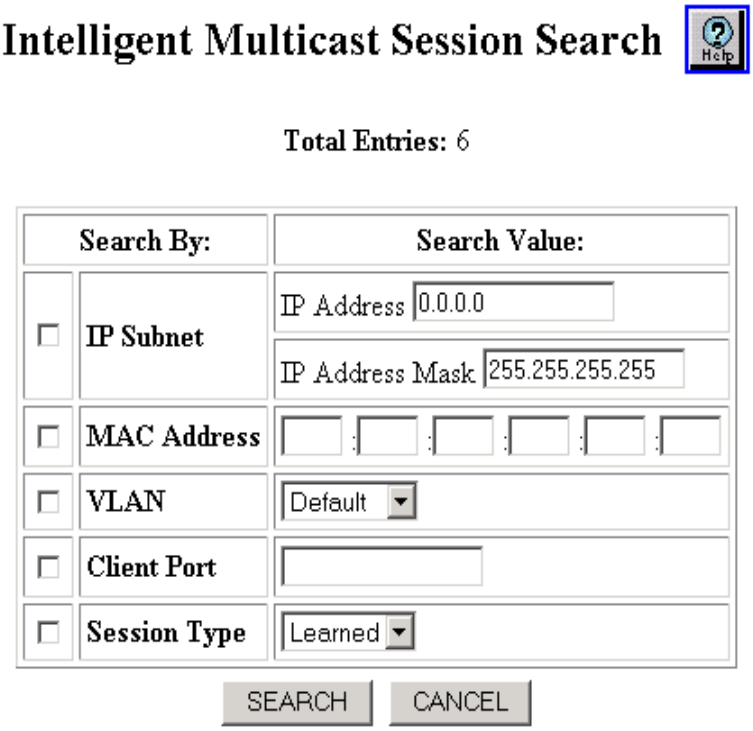
You can search for intelligent multicast sessions using either the Web Agent or the CLI.

### Using the Web Agent

To perform a session search using the Web Agent:

1. Select **Session Search** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **Intelligent Multicast Session Search** dialog box opens (Figure 6-147).

*Figure 6-147. Intelligent Multicast Session Search Dialog Box*



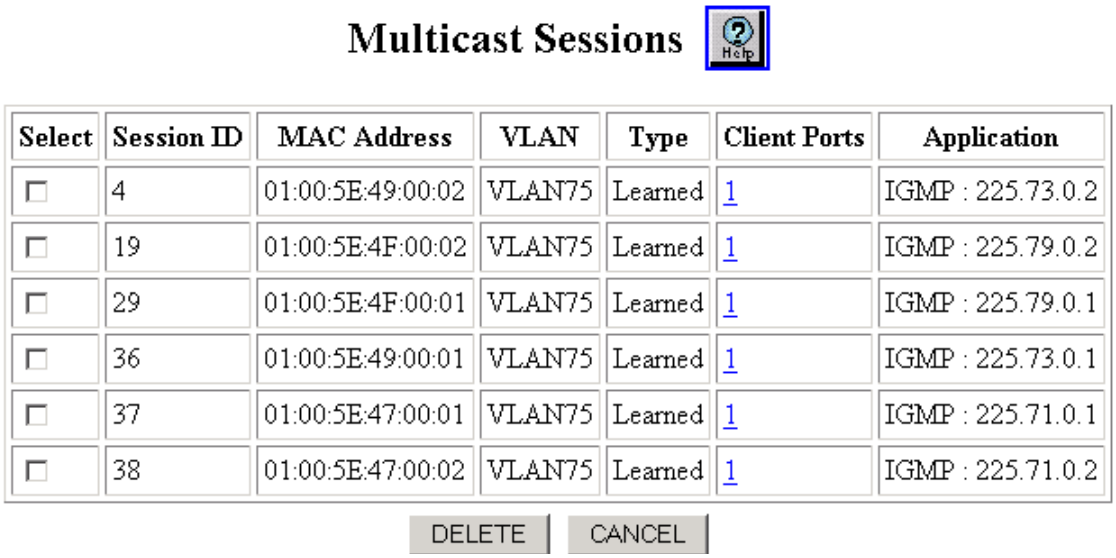

2. Refer to Table 2 for an explanation of the **Intelligent Multicast Session Search** dialog box parameters.

*Table 6-97. Intelligent Multicast Session Search Dialog Box Parameters*

| Search By Parameter: | Search Value: |
|---|---|
| **IP Subnet** | • I**P Address** - enter the IP address on which you want to perform a search<br>• **IP Address Mask** - Enter the associated IP Address mask |
| **MAC Address** | Enter the MAC address on which you want to perform a search |
| **VLAN** | Select a VLAN from the pull-down menu on which you want to perform a search. |
| **Client Port** | Enter a client port number on which you want to perform a search. |
| **Session Type** | Select a Session Type from the pull-down menu on which you want to perform a search. The options are Learned and Mgmt. |

3. Select **SEARCH** to begin the search for the multicast session. The **Multicast Sessions** dialog box opens with the search results (Figure 16-5).

*Figure 6-148. Multicast Sessions Dialog Box*




4. Refer to Table 6-98 for an explanation of the **Multicast Sessions** dialog box parameters:

*Table 6-98. Multicast Sessions Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Select** | Select the multicast session. |
| **Session ID** | Displays the multicast session identifier. |
| **MAC Address** | Displays the MAC address of the multicast session. |
| **VLAN** | Displays the VLAN on which the multicast session exists. |
| **Type** | Displays the type of multicast session. Options include:<br>• **Learned** - Entry is dynamically learned.<br>• **Mgmt** - Entry is configured statically by the user. |
| **Client Ports** | Displays the number of client ports in the multicast session and opens the Multicast Session Client Ports dialog box. |
| **Application** | Displays the active application(s) that configured the multicast session. The applications include:<br>• Mgmt<br>• IGMP<br>• LGMP<br>• CGMP |

### Using the CLI

To perform a session search using the CLI, enter the following command from User mode:

```
# show intelligent-multicast session <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Deleting an Intelligent Multicast Session

You can delete an intelligent multicast session using either the Web Agent or the CLI.

### Using the Web Agent

To delete an intelligent multicast session using the Web Agent:

1. Select **Session Search** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **Intelligent Multicast Session Search** dialog box opens (Figure 16-4).
2. Select **SEARCH** to begin the search for the multicast session. The **Multicast Sessions** dialog box opens with the search results (Figure 16-5).
3. Select the checkbox next to the multicast session that you want to delete and click **DELETE**.

*** Note:** Static (Mgmt) sessions can only be deleted through the Static Sessions dialog box.

### Using the CLI

To delete a multicast session using the CLI, enter the following command from Configure mode:

```
<configure># clear intelligent-multicast session
<session-id>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Deleting a Multicast Session Client Port

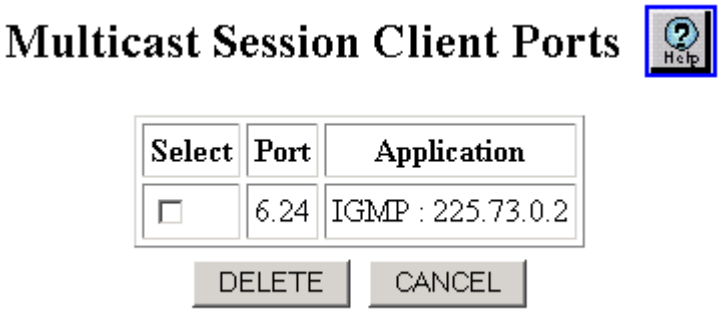
You can delete an intelligent multicast session client port by using either the Web Agent or the CLI.

## Using the Web Agent

To delete a multicast session client port by using the Web Agent:

1. Select **Session Search** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **Intelligent Multicast Session Search** dialog box opens (Figure 16-4).
2. Select **SEARCH** to begin the search for the multicast session. The **Multicast sessions** Dialog Box opens with the search results. (Figure 16-5)
3. Select the client port number from the **Client Ports** column. The **Multicast Session Client Port** dialog box opens.(Figure 16-6).

*Figure 6-149. Multicast Sessions Client Port*




4. Refer to Table 6-99 for an explanation of the **Multicast Session Client Port** dialog box parameters:

*Table 6-99. Multicast Session Client Port Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Select** | Select the multicast session client port. |
| **Port** | Displays the client port number. |
| **Application** | Displays the application(s) associated with this client port. The applications are:<br>• Mgmt<br>• IGMP<br>• LGMP<br>• CGMP |

5. Click **DELETE** to remove your selected multicast session client port, or **CANCEL** to restore previous settings.

*** Note:** Static (Mgmt) client ports can only be removed through the Static Sessions dialog box.

### Using the CLI

To delete a multicast session client port using the CLI, enter the following command from Configure mode:

```
<configure># clear intelligent-multicast client-
port <session-id> port <mod-port-spec>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Creating a Static Multicast Session

You can create a static multicast session using either the Web Agent or the CLI.

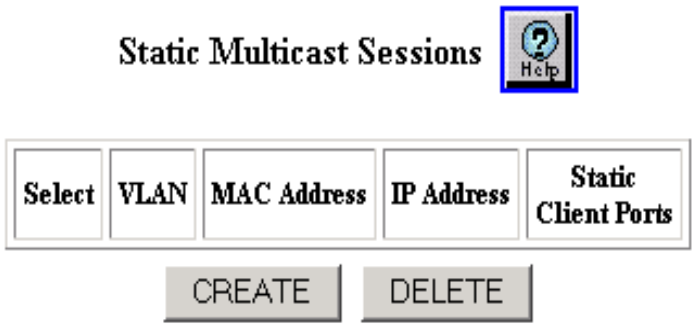
### Using the Web Agent

To create a new static multicast session using the Web Agent:

1. Select **Static Sessions** from **L2 > Intelligent Multicast** group on the Web Agent window. The **Static Multicast Sessions** dialog box opens (Figure 16-7).

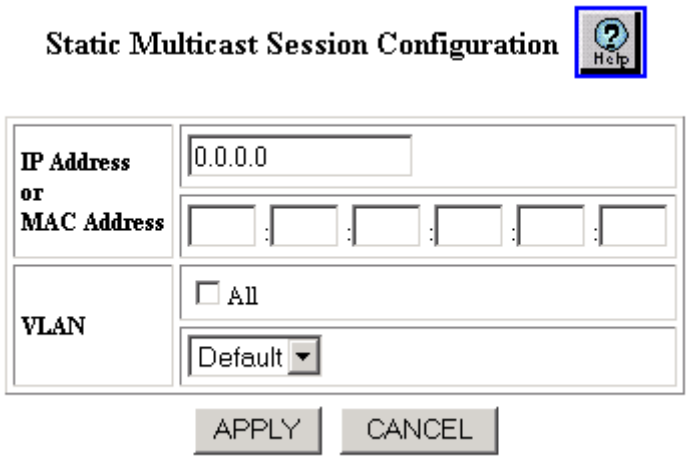
*** Note:** You must enable intelligent multicasting on a global basis to make your static multicast session active. See "Configuring Global Intelligent Multicasting", earlier in this chapter.

***Figure 6-150. Static Multicast Session Dialog Box***




2. Select **Create** to create a new session. The **Static Multicast Session Configuration** dialog box opens (Figure 16-8).

*Figure 6-151. Static Multicast Session Configuration Dialog Box*




3. Configure the **Static Multicast Session Configuration** dialog box parameters (refer to Table 6-100):

*Table 6-100. Static Multicast Session Configuration Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **IP Address** | Enter the IP address of the new static multicast session. The range must be between 224.0.1.0 to 239.255.255.255. |
| **MAC Address** | Enter the MAC address of the new static multicast session. Specifying the MAC address is not used for an IP multicast session. |
| **VLAN** | Enter the VLAN associated with the new multicast session. Click All to add all VLANs to the multicast session, or select a specific VLAN from the pull-down menu. |

4. Click **APPLY** to create the new static multicast session, or **CANCEL** to restore previous settings.

### Using the CLI

To create a new static multicast session using the CLI, enter the following command from Configure mode:

```
<configure># set intelligent-multicast
static-session <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Deleting Static Multicast Sessions

You can delete static multicast sessions using either the Web Agent or the CLI.

### Using the Web Agent

To delete a static multicast session using the Web Agent:

1. Select **Static Sessions** from **L2 > Intelligent Multicast** group on the Web Agent window. The **Static Multicast Sessions** dialog box opens (Figure 6-152).
2. Refer to Table 6-101 for an explanation of the **Static Multicast Sessions** dialog box parameters.

***Figure 6-152. Static Multicast Sessions Dialog Box***

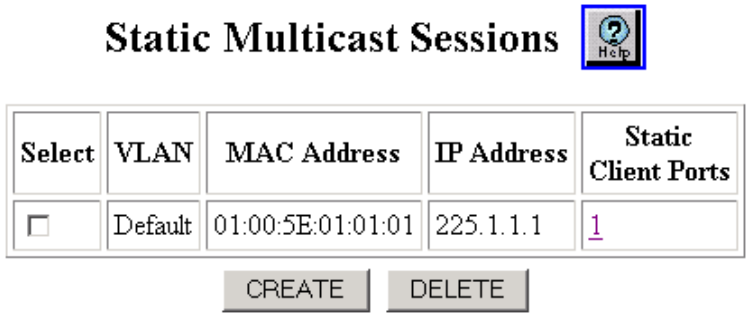


*Table 6-101. Static Multicast Sessions Dialog Box*

| Parameter | Definition |
|---|---|
| **Select** | Select the static multicast session to be deleted. |
| **VLAN** | Displays the VLAN on which the static multicast session exists. |
| **MAC Address** | Displays the MAC address of the static multicast session. |
| **IP Address** | Displays the IP address associated with the static multicast session, if available. |
| **Static Client Ports** | Displays the number of static client ports associated with the static multicast session and opens the Static Multicast Session Client Ports dialog box. |

3. Select the checkbox next to the static multicast session that you want to delete.

4. Click **DELETE** to remove the static multicast session.

### Using the CLI

To delete a static multicast session using the CLI, enter the following command from Configure mode:

```
<configure># clear intelligent-multicast
static-session <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Creating Static Client Ports

You can create and add static client ports using either the Web Agent or the CLI.

*** Note:** You can only add static client ports to static sessions on VLANs that the port is bound to or on sessions created for All VLANs.

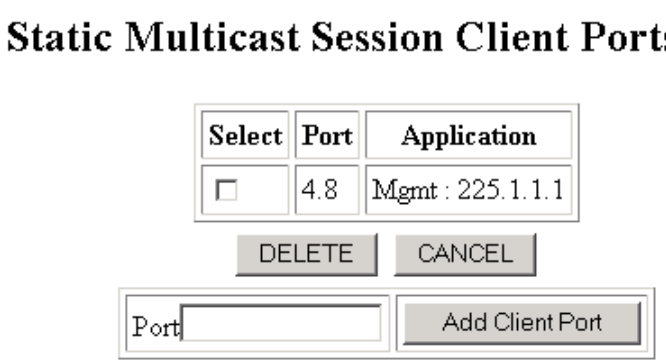
### Using the Web Agent

To create a static client port using the Web Agent:

1. Select **Static Sessions** from **L2 > Intelligent Multicast** group on the Web Agent window. The **Static Multicast Sessions** dialog box opens (Figure 6-152).

2. Select the number from the **Static Client Ports** column. The **Static Multicast Sessions Client Ports** dialog box opens (Figure 6-153).

*Figure 6-153. Static Multicast Sessions Clients Port Dialog Box*




3. Enter the new port number to be added in the **Port** field,.
4. Click **Add Client Port**. The new port is added.

### Using the CLI

To create a static client port using the CLI, enter the following command from Configure mode:

```
(configure)# set intelligent-multicast static-
client-port <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Deleting Static Client Ports

Static client ports can be deleted from either the Web or the CLI.

### Using the Web Agent

To delete static client ports using the Web Agent:

1. Select **Static Sessions** from **L2 > Intelligent Multicast** group on the Web Agent window. **The Static Multicast Sessions** dialog box opens (Figure 6-152).
2. Select the number from the **Static Client Ports** column. The **Static Multicast Sessions Client Ports** dialog box opens (Figure 6-153).
3. Select a port and click **DELETE** to remove the static client port, or **CANCEL** to restore previous settings.

### Using the CLI

To delete static client ports using the CLI, enter the following command from Configure mode:

```
<configure># clear intelligent-multicast static-
client-port <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Managing Internet Group Management Protocol (IGMP) Snooping

This section provides the following procedures:

- Enabling IGMP Snooping
- Viewing IGMP Snooping Statistics

*Figure 6-154. IGMP Snooping Dialog Box*

*Table 6-102. IGMP Snooping Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Enable State** | Select **Enable** to allow the IGMP snooping on the interface. The default value is **Disable**. |
| **Intelligent Multicast Session Statistics** | • **New Sessions Created** - Displays the number of new sessions created by IGMP snooping.<br>• **Sessions Destroyed** - Displays the number of sessions removed by IGMP snooping.<br>• **New Client Ports Added** - Displays the number of new client ports added by IGMP snooping.<br>• **New Router Ports Added** - Displays the number of new router ports added by IGMP snooping.<br>• **Router Ports Removed** - Displays the number of router ports removed by IGMP snooping. |

# Enabling IGMP Snooping

You can enable IGMP snooping using either the Web Agent or the CLI.

## Using the Web Agent

To enable IGMP Snooping using the Web Agent:

1. Select **IGMP Snooping** from the L2 > **Intelligent Multicast group** on the Web Agent window. The **IGMP Snooping** dialog box opens (Figure 16-11).

*** Note:** IGMP snooping only works on VLANS that have an IGMP interface enabled. You must also enable intelligent multicasting on a global basis.

2. Select **Enable** from the State field.
3. Click **APPLY** to complete the operation or **CANCEL** to ignore the operation.

## Using the CLI

To enable IGMP Snooping using the CLI, enter the following command from Configure mode:

```
(configure)# set igmp-snooping enable
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Viewing IGMP Snooping Statistics

You can view IGMP snooping statistics using either the Web Agent or the CLI.

## Using the Web Agent

To view IGMP snooping using the Web Agent:

1. Select **IGMP Snooping** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **IGMP Snooping** dialog box opens (Figure 16-11).
2. Refer to Table 6-102 for an explanation of the **IGMP Snooping** dialog box parameters:
3. Click:
   - **CLEAR** to clear the statistics.
   - **REFRESH** to refresh the contents of the table.

### Using the CLI

To configure IGMP snooping using the CLI, enter the following command from Configure mode:

```
(configure)# show igmp-snooping statistics
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Managing the Lucent Group Management Protocol (LGMP) Server

The section provides the following procedures:

- Configuring the LGMP Server
- Viewing the LGMP Server Statistics
- Viewing the LGMP Server Statistics per VLAN

*Figure 6-155. LGMP Server Configuration Dialog Box*

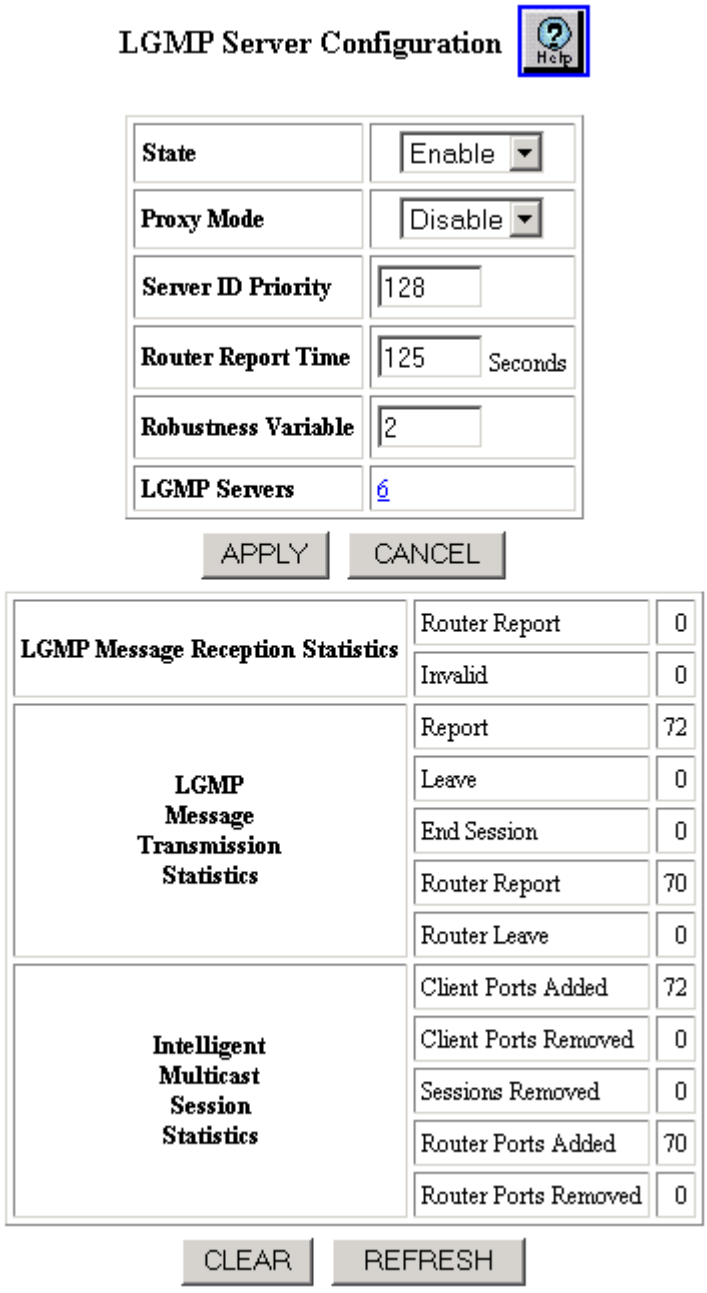


*Table 6-103. LGMP Server Configuration Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Enable State** | Select to enable or disable LGMP server configuration. The default value is Disabled. |
| **Proxy Mode** | Select to enable or disable Proxy mode. Proxy mode allows the server to send LGMP router report and leave messages on behalf of neighbor routers on the same VLAN. |
| **Server ID Priority** | The priority of the LGMP server on this switch. The server ID priority and the IP address associated with the VLAN determine whether the LGMP server wins LGMP distribution election. The lower the number the more likely it will win the election. The valid range is 0 to 255. The default value is 128. |
| **Router Report Time** | The time interval (in seconds) between router reports sent by the LGMP server in distributor state. The valid range is 10 to 10,000. The default value is 125 seconds. |
| **Robustness Variable** | The scalar value used by non-distributor LGMP servers when timing out the LGMP server in the distributor state. The valid range is 2 to 10. The default value is 2. |
| **LGMP Servers** | Displays the number of LGMP servers and opens the LGMP Server Display per VLAN dialog box.<br>**Note: Only VLANs that have an active IGMP interface can be LGMP servers.** |
| **LGMP Message Reception Statistics** | • **Router Report** - Displays the number of LGMP router report messages received.<br>• **Invalid** - Displays the number of LGMP messages received with an invalid payload. |

| Parameter | Definition |
|---|---|
| **LGMP Message Transmission Statistics** | • **Report** - Displays the number of LGMP report messages transmitted.<br>• **Leave** - Displays the number of LGMP leave messages transmitted.<br>• **End Session** - Displays the number of LGMP end session messages transmitted.<br>• **Router Report** - Displays the number of LGMP router report messages transmitted.<br>• **Router Leave** - Displays the number of LGMP router leave messages transmitted. |
| **Intelligent Multicast Session Statistics** | • **Client Ports Added**- Displays the number of add client events generated by LGMP.<br>• **Client Ports Removed** - Displays the number of remove client events generated by LGMP.<br>• **Sessions Removed**- Displays the number of remove session events generated by LGMP.<br>• **Router Ports Added**- Displays the number of add router events generated by LGMP.<br>• **Router Ports Removed**- Displays the number of remove router events generated by LGMP. |

# Configuring the LGMP Server

You can configure the LGMP server using either the Web Agent or the CLI.

## Using the Web Agent

To configure the LGMP server using the Web Agent:

1. Select **LGMP Server** from the L2 > **Intelligent Multicast** group on the Web Agent window. The **LGMP Server Configuration** dialog box opens (Figure 16-12).

   *** Note:** You must enable intelligent multicasting on a global basis to activate the LGMP Server. LGMP serving is only active on VLANs with an IGMP interface enabled and IGMP snooping globally enabled.

2. Refer to Table 6-103 to configure the **LGMP Server Configuration** dialog box parameters.

3. Click...
   - **APPLY** to save your changes.
   - **CANCEL** to restore previous settings.

### Using the CLI

To configure the LGMP server using the CLI, enter the following command from **Configure** mode:

```
<configure># set lgmp server <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Viewing the LGMP Server Statistics

You can view the LGMP server statistics using either the Web Agent or the CLI.

### Using the Web Agent

To enable/view the LGMP server using the Web Agent:

1. Select **LGMP Snooping** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **LGMP Server Configuration** dialog box opens (Figure 16-12).
2. Select **Enable** from the **State** field, if it is not already displayed.
3. Click **CLEAR** to clear the statistics or **REFRESH** to refresh the contents of the table.

### Using the CLI

To view the LGMP server statistics using the CLI, enter the following command from Configure mode:

```
<configure># show lgmp server statistics
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Viewing the LGMP Server Statistics per VLAN

You can view the LGMP server statistics per VLAN using either the Web Agent or the CLI.

## Using the Web Agent

To modify the LGMP server display per VLAN using the Web Agent:

1. Select **LGMP Server** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **LGMP Server** Select the number from the **LGMP Servers** column. The **LGMP Server Display per VLAN** dialog box opens (Figure 16-13).

*** Note:** You must enable intelligent multicasting on a global basis to activate your LGMP server per VLAN configuration

2. Select the number from the **LGMP Servers** column. The **LGMP Server Display** dialog box opens (Figure 16-13)

3. Refer to Table 6-104 to configure the **LGMP Server Display per VLAN.**

***Figure 6-156. LGMP Server per VLAN Dialog Box.***

LGMP Server Display per VLAN

| Select | VLAN | State | LGMP Message Reception Statistics | | LGMP Message Transmission Statistics | | | | | Intelligent Multicast Session Statistics | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Router Report | Invalid | Report | Leave | End Session | Router Report | Router Leave | Client Ports Added | Client Ports Removed | Sessions Removed | Router Ports Added | Router Ports Removed |
| ☐ | VLAN34 | Distributor | 0 | 0 | 0 | 0 | 0 | 15 | 0 | 0 | 0 | 0 | 15 | 0 |
| ☐ | VLAN52 | Distributor | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 |
| ☐ | VLAN54 | Distributor | 0 | 0 | 0 | 0 | 0 | 16 | 0 | 0 | 0 | 0 | 16 | 0 |
| ☐ | VLAN55 | Distributor | 0 | 0 | 0 | 0 | 0 | 16 | 0 | 0 | 0 | 0 | 16 | 0 |
| ☐ | VLAN74 | Distributor | 0 | 0 | 0 | 0 | 0 | 15 | 0 | 0 | 0 | 0 | 15 | 0 |
| ☐ | VLAN75 | Distributor | 0 | 0 | 90 | 0 | 0 | 15 | 0 | 90 | 0 | 0 | 15 | 0 |

CLEAR CLEAR ALL REFRESH

***Table 6-104. LGMP Server Display per VLAN Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Select** | Select the LGMP server to modify. |
| **VLAN** | Displays the VLAN associated with the LGMP server. |

*Table 6-104. LGMP Server Display per VLAN Dialog Box Parameters*
*continued*

| Parameter | Definition |
|---|---|
| **State** | Displays the current state of the LGMP server.<br>• **Distributor** - The LGMP server serves LGMP messages to LGMP clients.<br>• **Non-Distributor** - The LGMP server monitors the current distributor. |
| **LGMP Message Reception Statistics** | • **Router Report** - Displays the number of LGMP router report messages received per VLAN.<br>• **Invalid** - Displays the number of LGMP messages received with an invalid payload per VLAN. |
| **LGMP Messages Transmission Statistics** | • **Report** - Displays the number of LGMP report messages transmitted per VLAN.<br>• **Leave** - Displays the number of LGMP leave messages transmitted per VLAN.<br>• **End Session** - Displays the number of LGMP end session messages transmitted per VLAN.<br>• **Router Report** - Displays the number of LGMP router report messages transmitted per VLAN.<br>• **Router Leave** - Displays the number of LGMP router leave messages transmitted per VLAN. |
| **Intelligent Multicast Session Statistics** | • **Client Ports Added**- Displays the number of add client events generated by LGMP per VLAN.<br>• **Client Ports Removed**- Displays the number of remove client events generated by LGMP per VLAN.<br>• **Sessions Removed**- Displays the number of remove session events generated by LGMP per VLAN.<br>• **Router Ports Added**- Displays the number of add router events generated by LGMP per VLAN.<br>• **Router Ports Removed**- Displays the number of remove router events generated by LGMP per VLAN. |

4. Click:

   — **CLEAR** to reset selected row information.

— **CLEAR ALL** to reset all statistics.

— **REFRESH** to view the latest information

### Using the CLI

To view the LGMP server statistics per VLAN using the CLI, enter the following command from Configure mode:

```
<configure># show lgmp server statistics VLAN
options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Managing the Lucent Group Management Protocol (LGMP) Client

This section provides the following procedures:

- Enabling the LGMP Client
- Viewing LGMP Clients per VLAN statistics

*Figure 6-157. LGMP Client Configuration Dialog Box*

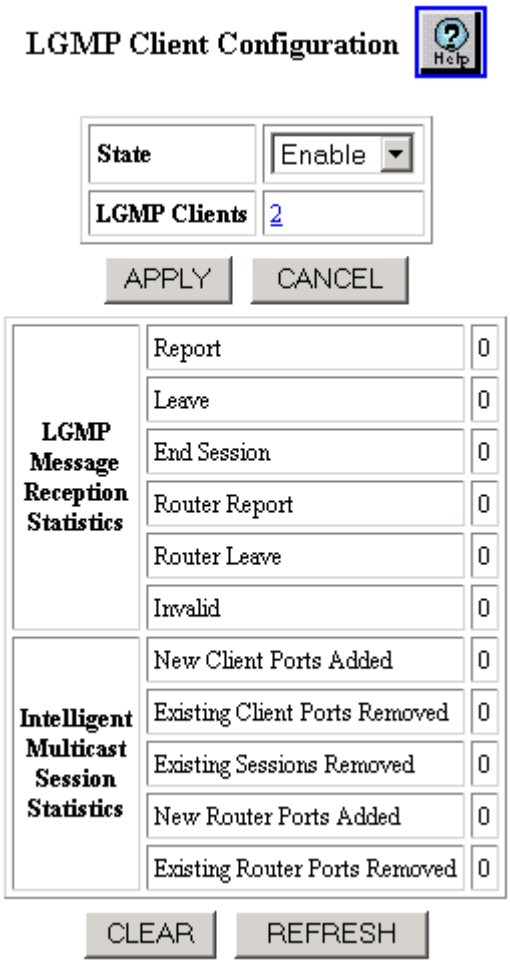


*Table 6-105. LGMP Client Configuration Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Enable State** | Select to enable or disable LGMP client. The default value is Disabled. |
| **LGMP Clients** | Displays the number of LGMP clients per VLAN and opens the LGMP Client Displays per VLAN dialog box. |
| **LGMP Message Reception Statistics** | • **Report** - Displays the number of LGMP report messages received.<br>• **Leave** - Displays the number of LGMP leave messages received.<br>• **End Session** - Displays the number of LGMP end session messages received.<br>• **Router Report** - Displays the number of LGMP router report messages received.<br>• **Router Leave** - Displays the number of LGMP router leaves messages received.<br>• **Invalid** - Displays the number of LGMP messages received with an invalid payload. |
| **Intelligent Multicast Session Statistics** | • **New Client Ports Added** - Displays the number of new clients added by LGMP.<br>• **Existing Client Ports Removed** - Displays the number of clients removed by LGMP.<br>• **Existing Sessions Removed** - Displays the number of sessions removed by LGMP.<br>• **New Router Ports Added** - Displays the number of new routers added by LGMP.<br>• **Existing Router Ports Removed** - Displays the number of new routers removed by LGMP. |

# Enabling the LGMP Client

You can enable the LGMP client statistics using either the Web Agent or the CLI.

## Using the Web Agent

To enable an LGMP client using the Web Agent:

1. Select **LGMP Client** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **LGMP Client Configuration** dialog box opens (Figure 6-157).

*** Note:** You must enable intelligent multicasting on a global basis to activate LGMP client configuration.

2. Select **Enable** from the State field pull-down menu, if it is not already displayed.
3. Select **APPLY** to complete the operation, or **CANCEL** to ignore the operation.

### Using the CLI

To enable an LGMP client using the CLI, enter the following command from Configure mode:

```
<configure># set lgmp client enable
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Viewing LGMP Clients Statistics

You can view LGMP clients statistics using either the web agent or the CLI.

### Using the Web Agent

To view LGMP Client statistics using the web:

1. Select **LGMP Client** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **LGMP Client Configuration** dialog box opens (Figure 6-157).
2. Refer to Table 6-105 for an explanation of the LGMP Client Configuration dialog box parameters
3. Click **CLEAR** to clear the statistics, or **REFRESH** to refresh the contents of the table.

### Using the Web

To view LGMP Client statistics using the CLI:

To view the LGMP client statistics using the CLI, enter the following command from Configure mode:

```
<configure># show lgmp client statistics
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Viewing LGMP Clients per VLAN statistics

You can view LGMP clients per VLAN statistics using either the web agent or the CLI.

***Figure 6-158. LGMP Client Display per VLAN Dialog Box***

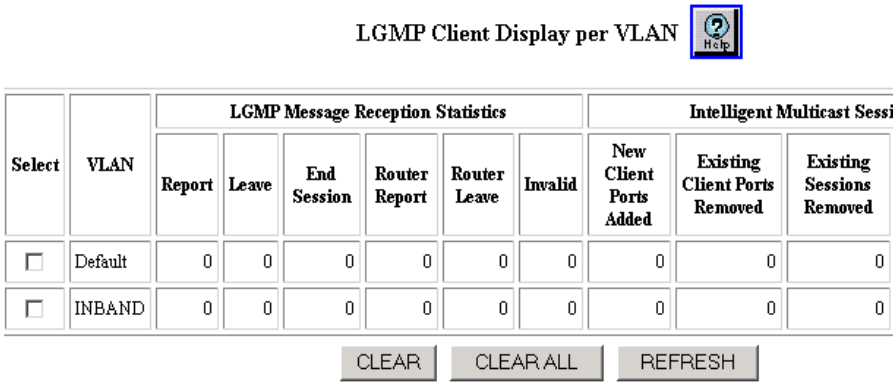



***Table 6-106. LGMP Client Display per VLAN Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Select** | Select the LGMP client statistics to clear. |
| **VLAN** | Displays the VLAN associated with the LGMP client. |
| **LGMP Message Reception Statistics** | • **Report** - Displays the number of LGMP report messages received per VLAN.<br>• **Leave** - Displays the number of LGMP leave messages received per VLAN.<br>• **End Session** - Displays the number of LGMP end session messages received per VLAN.<br>• **Router Report** - Displays the number of LGMP router report messages received per VLAN.<br>• **Router Leave** - Displays the number of LGMP router leaves messages received per VLAN.<br>• **Invalid** - Displays the number of LGMP messages received with an invalid payload per VLAN. |

| Parameter | Definition |
|---|---|
| **Intelligent Multicast Session Statistics** | • **New Client Ports Added** - Displays the number of new clients added by LGMP per VLAN.<br>• **Existing Client Ports Removed** - Displays the number of clients removed by LGMP per VLAN.<br>• **Existing Sessions Removed** - Displays the number of sessions removed by LGMP per VLAN.<br>• **New Router Ports Added** - Displays the number of new routers added by LGMP per VLAN.<br>• **Existing Router Ports Removed** - Displays the number of new routers removed by LGMP per VLAN. |

## Using the Web Agent

To view LGMP client statistics per VLAN using the Web Agent:

1. Select **LGMP Client** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **LGMP Client Configuration** dialog box opens (Figure 6-157).
2. Select the number from the **LGMP Clients** field. The **LGMP Client Display per VLAN** dialog box opens (Figure 16-15).
3. Refer to Table 6-106 for an explanation of the **LGMP Client Display per VLAN** dialog box parameters.
4. Click...
   - **CLEAR** to reset selected row information.
   - **CLEAR ALL** to reset all statistics.
   - **REFRESH** to view the latest information.

## Using the CLI

To modify LGMP client statistics per VLAN using the CLI, enter the following command in Configure mode:

```
<configure># show lgmp client statistics VLAN
<options>
```

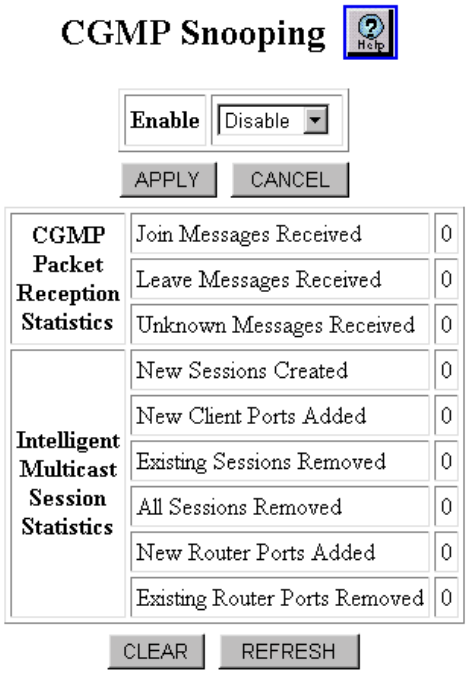
Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Managing Cisco Group Management Protocol (CGMP) Snooping

You can manage CGMP snooping by using either the Web Agent or the CLI. This section provides the following procedures:

- Enabling CGMP Snooping
- Viewing CGMP Snooping

***Figure 6-159. CGMP Snooping Dialog Box***




## Enabling CGMP Snooping

You can enable CGMP Snooping using either the web agent or the CLI.

### Using the Web Agent

To enable CGMP snooping using the Web Agent:

1. Select **CGMP Snooping** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **CGMP Snooping** dialog box opens (Figure 16-16).

*** Note:** You must enable intelligent multicasting on a global basis to activate CGMP snooping configuration.

2. Refer to Table 6-107 for an explanation of the CGMP Snooping dialog box parameters.

***Table 6-107. CGMP Snooping Dialog Box Parameters***

| Parameter | Definition |
|---|---|
| **Enable State** | Select to enable or disable CGMP snooping. |
| **CGMP Packet Reception Statistics** | • **Join Messages Received** - Displays the number of CGMP join messages received.<br>• **Leave Messages Received** - Displays the number of CGMP leave messages received.<br>• **Unknown Messages Received** - Displays the number of unknown CGMP messages received. |
| **Intelligent Multicast Session Statistics** | • **New Sessions Created** - Displays the number of new multicast sessions created by CGMP snooping.<br>• **New Client Ports Added** - Displays the number of new client ports added to a multicast session.<br>• **Existing Sessions Removed** - Displays the number of existing multicast sessions that have been removed by CGMP snooping.<br>• **All Sessions Removed** - Displays the number of times that all multicast sessions created by CGMP snooping were removed.<br>• **New Router Ports Added** - Displays the number of new router ports added by CGMP snooping.<br>• **Existing Router Ports Removed** - Displays the number of router ports that were created by the CGMP snooper and were removed. |

3. Click...
   - **APPLY** to save your changes
   - **CANCEL** to restore previous settings.

## Using the CLI

To enable CGMP snooping using the CLI, enter the following command from Configure mode:

```
<configure># set cgmp enable
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Viewing CGMP Snooping

You can view CGMP Snooping using either the web agent or the CLI.

## Using the Web Agent

To view CGMP snooping using the Web Agent:

1. Select **CGMP Snooping** from the **L2 > Intelligent Multicast** group on the Web Agent window. The **CGMP Snooping** dialog box opens (Figure 6-159).
2. View the CGMP Snooping dialog box fields.
3. Click:
   - **CLEAR** to clear the statistics
   - **REFRESH** to refresh the contents of the table

## Using the CLI

To view CGMP snooping using the CLI, enter the following command from User mode:

```
># show cgmp statistics <options>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# 17 Monitoring the Avaya Multiservice Switch

## Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:

- Interpreting Front Panel LED Displays
- Checking Temperature Status and Configuring Thresholds
- Checking Active Alarms
- Using the Event Subsystem
- Setting Log Size

## Interpreting Front Panel LED Displays

*Refer to Table 6-108* for an explanation of the Avaya P550R/P580/P880/P882 switch front-panel LEDs:

***Table 6-108. Front Panel LED Display Interpretation***

| Module... | LED... | Behavior... | Indication... |
|---|---|---|---|
| All Modules | Module Status | Solid green | Normal operation. |
| | | Flashing orange | Diagnostic failure. |
| | | Off | Module not operational or not receiving power. |
| Gigabit Modules | TX/RX | Flashing orange | Port sending/receiving traffic. |
| | | Off | Port not sending/receiving traffic. |
| | Port | Solid green | Port enabled with link up. |
| | | Flashing green | Port disabled. |
| | | Flashing orange | Hardware failure. |
| | | Off | No link. |

*Table 6-108. Front Panel LED Display Interpretation continued*

| Module... | LED... | Behavior... | Indication... |
|---|---|---|---|
| 10/100 Modules | Port | Solid green, with orange flash | Port enabled and sending and receiving traffic Traffic indicated by yellow flashes. |
| | | Flashing green | Port disabled with link up. |
| | | Flashing orange | Hardware failure. |
| | | Off | No link. |

## Checking Temperature Status and Configuring Thresholds

You can check the temperature status and configure temperature thresholds by using either the Web Agent or the CLI.

*** Note:** The temperature thresholds have been raised for the backplane and slot 1. In high temperature climates, the switch was frequently reaching the default temperature thresholds. Table 6-109 lists the new default temperature thresholds. All temperatures are measured in degrees Celsius.

*Table 6-109. New Default Temperature Thresholds*

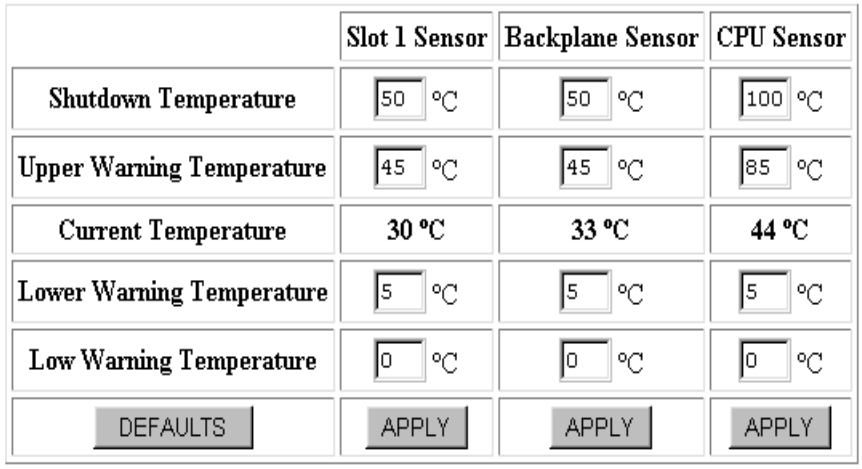
| Temperature Threshold | Slot 1 | Backplane | CPU Sensor |
|---|---|---|---|
| Upper Warning | 60° | 60° | 85° |
| Lower Warning | 5° | 5° | 5° |
| Low Warning | 0° | 0° | 0° |
| Shutdown Temperature | 65° | 65° | 100° |

## Using the Web Agent

To check the temperature status and configure thresholds from the Web Agent:

1. Select T**emperature system** from the **System > Configuration** group on the Web Agent windows. The **Temperature System** dialog box (Figure 6-108) opens.

***Figure 6-160. Temperature System Dialog Box (M5500-SupA, M550R, M880R)***




*** Note:** The P880 does not display the current temperature of the backplane. In the **Current Temperature** field, the switch displays `--`.

If a redundant Supervisor module is installed, the **Slot 2 Sensor** column displays.

You cannot change settings for the backplane temperature sensors on the P880. If you attempt to change the settings, the switch displays the following error message:

```
Set Limits for Backplane Sensor failed -
failure writing to sensor
```

2. Refer to Table 6-110 to set the threshold values:

***Table 6-110. Temperature Threshold Values***

| Threshold | Defines... |
|---|---|
| **Shutdown Temperature** | Value in degrees Celsius that causes the switch to send a trap to the network management station and triggers a shutdown when it is passed. The default value is 100 degrees Celsius. |
| **Upper Warning Temperature** | Value in degrees Celsius that causes the switch to send a high temperature threshold warning when it is passed. The default value is 85 degrees Celsius. |
| **Lower Warning Temperature** | Value that in degrees Celsius that when passed causes the switch to send a warning that the temperature is approaching the low temperature threshold. By default, this value is 5 degrees Celsius. |
| **Low Shutdown Temperature** | Indicates the low shutdown temperature for a switch to reset the warning and high thresholds. This value prevents the switch from sending traps continually if the temperature is hovering around the threshold value. The default value is 0 degrees Celsius. |

## Using the CLI

To check the temperature status using the CLI, enter the following command from **Configuration** mode:

```
<configure># show temperature
```

To Configure temperature threshold values using the CLI, enter the following command from **Configuration) mode**:

```
<configure># set temperature <options (backplane
sensor, CPU-sensor, probe, supervisor-slot)>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about these commands.

# Checking Active Alarms

Each switch stores a table of active alarms from which you can view a list of open issues without having to view the entire event log. This provides you with a quick snapshot of the switch's health.

This section provides the following procedures:

- Viewing the Active Alarm Table
- Using the Event Subsystem
- Configuring the Protocol Event Log
- Viewing the Event and Shutdown Logs
- Viewing Event Statistics

## Viewing the Active Alarm Table

You can view the active alarm table using either the Web Agent or the CLI.

### Using the Web Agent

To view the **Active Alarm Table** using the Web Agent:

1. Select **Active Alarms** from the Events group on the Web Agent window. The **Active Alarm Table** opens (Figure 6-161).

***Figure 6-161. Active Alarm Table Dialog Box***

**Active Alarm Table**

| ID | Name | Value | Owner |
|---|---|---|---|
| 10 | Port Status | No Link | Port 2.1 |
| 11 | Port Status | No Link | Port 2.2 |
| 12 | Port Status | No Link | Port 2.3 |
| 13 | Port Status | No Link | Port 2.4 |
| 14 | Port Status | No Link | Port 2.5 |
| 15 | Port Status | No Link | Port 2.6 |
| 16 | Port Status | No Link | Port 2.7 |
| 17 | Port Status | No Link | Port 2.8 |
| 18 | Port Status | No Link | Port 2.9 |
| 19 | Port Status | No Link | Port 2.10 |
| 20 | Port Status | No Link | Port 2.11 |
| 21 | Port Status | No Link | Port 2.12 |
| 22 | Port Status | No Link | Port 3.1 |
| 23 | Port Status | No Link | Port 3.2 |
| 24 | Port Status | No Link | Port 3.3 |

### Using the CLI

To view the **Active Alarm Table** using the CLI, enter the following command from **Configuration** mode:

```
<configure># show alarms
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Using the Event Subsystem

There are two switch system activity logs:

- **Event Log** - stores a large table of events. The size of the table is user-settable. Because these events are stored in switch memory, the list is cleared each time the switch reboots.
- **Shutdown Log** - stores the same information as the Event Log, but generally in a smaller table because the table is stored in the switch's nonvolatile RAM (NVRAM). This log list is particularly useful in assessing the cause of a switch failure, because the information is retained even after the switch restarts.

*** Note:** The following events are now logged in the event log:

- Toggling between the primary and redundant switch controller or switch element.
- Full functioning of the redundant supervisor after a failure of the primary supervisor.

# Configuring the Protocol Event Log

You can use the protocol event log to enable RIP and OSPF packet tracing for layer 3 only. RIP requests and responses received and sent through all RIP interfaces are logged to the event log as protocol events. OSPF packet types received and sent through all OSPF interfaces are logged to the event log as protocol events. AppleTalk packet types received and sent through all AppleTalk interfaces are logged to the event log as protocol events. LDAP packet types received and sent through all LDAP interfaces are logged to the event log as protocol events.

*** Note:** Enabling the protocol event log may cause the event log to be rapidly filled with protocol events.

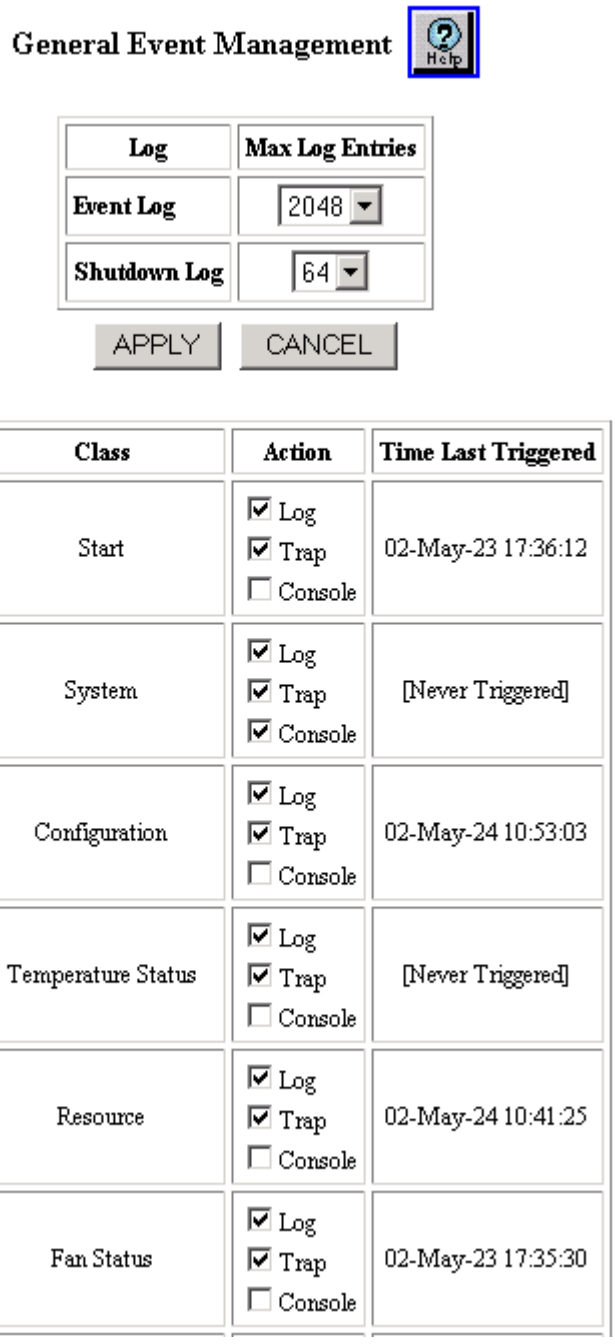
You can Configure the protocol event log using either the Web Agent or the CLI.

## Using the Web Agent

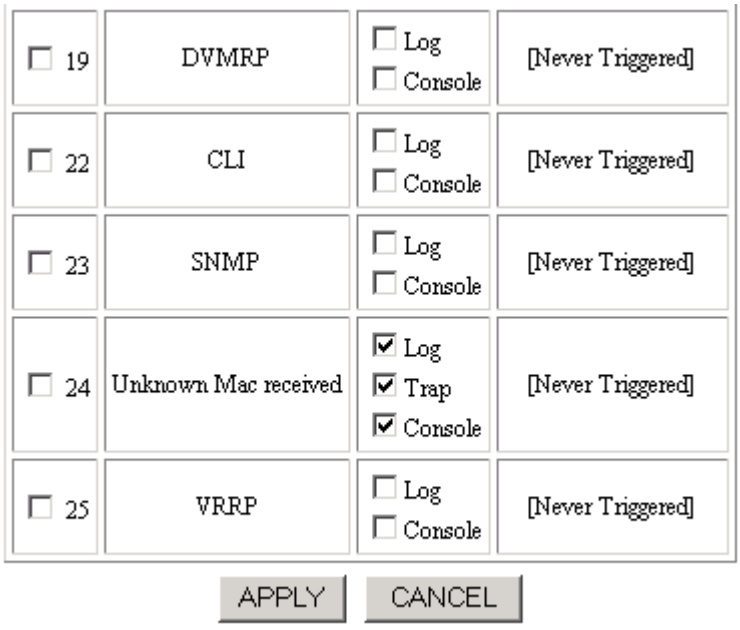
To Configure the protocol event log using the Web Agent:

1. Select **General Events** from the **Events** group on the Web Agent window. The **General Event Management** dialog box opens (Figure 6-162).

*Figure 6-162. General Event Management Dialog Box (3-Parts)*

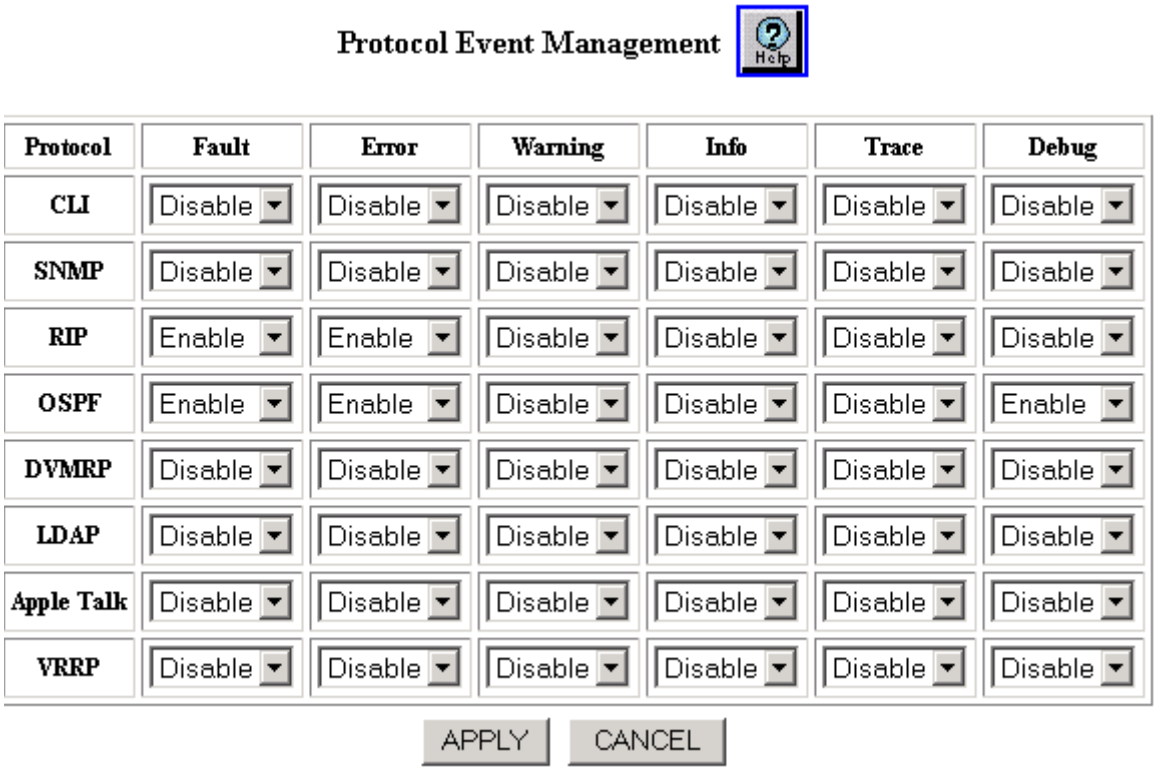


| | | | |
|---|---|---|---|
| ☐ 7 | Service Port Status | ☑ Log<br>☑ Trap<br>☐ Console | 02-May-24 10:41:25 |
| ☐ 8 | User Port Status | ☑ Log<br>☐ Trap<br>☐ Console | [Never Triggered] |
| ☐ 9 | Authentication Failure | ☑ Log<br>☑ Trap<br>☐ Console | 02-May-23 17:35:29 |
| ☐ 10 | Bridge Status | ☑ Log<br>☑ Trap<br>☐ Console | 02-May-23 17:36:14 |
| ☐ 11 | Switch Fabric | ☑ Log<br>☑ Trap<br>☑ Console | [Never Triggered] |
| ☐ 12 | OSPF | ☑ Log<br>☐ Console | 02-May-28 09:53:36 |
| ☐ 13 | RIP | ☐ Log<br>☑ Console | [Never Triggered] |
| ☐ 14 | LDAP | ☐ Log<br>☐ Console | [Never Triggered] |
| ☐ 15 | Appletalk | ☐ Log<br>☐ Console | [Never Triggered] |
| ☐ 16 | Power Status | ☑ Log<br>☑ Trap<br>☐ Console | [Never Triggered] |
| ☐ 18 | Redundant CPU | ☑ Log<br>☑ Trap<br>☐ Console | 02-May-23 17:35:30 |




2. Select one of the following from the **ID** column:
   - CLI
   - SNMP
   - RIP
   - OSPF
   - DVMRP
   - LDAP
   - AppleTalk
   - VRRP
3. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.
4. Select **Protocol Events** from the **Events** group on the web page window. The **Protocol Event Management** dialog box opens (Figure 6-163).

*Figure 6-163. Protocol Event Management Dialog Box*




5. Refer to Table 6-111 to Configure the Protocol Event Management dialog box parameters for the specific protocols that you have Configured on your switch:

*Table 6-111. Protocol Event Management Dialog Box Parameters*

| Column Heading | Parameter |
|---|---|
| **Fault** | Select **Enable** to display serious errors that can cause a system crash, for example, panic. The default is **Disable**. |
| **Error** | Select **Enable** to display serious errors that will not cause a system crash but can contribute protocol problems. |
| **Warning** | Select **Enable** to display non-critical errors. The default is **Disable**. |
| **Info** | Select **Enable** to display Event details. The default is **Disable.** |

*Table 6-111. Protocol Event Management Dialog Box Parameters*
*continued*

| Column Heading | Parameter |
|---|---|
| **Trace** | Select **Enable** to display RIP and OSPF packet tracing. The default is **Disable**. |
| **Debug** | Select **Enable** to display event messages used to troubleshoot a network problem. The default is **Disable**. |

6. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

### Using the CLI

To configure the protocol event log using the CLI, enter the following command from **Configuration** mode:

```
<configure># logging protocol event <protocol>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Viewing the Event and Shutdown Logs

You can view the Event and Shutdown logs using either the Web Agent or the CLI.

### Using the Web Agent

To view the Event and Shutdown logs using the Web Agent:

1. Select either **Event Log** or **Shutdown Log** from the **Events** group on the Web Agent window. The **Event Log Search** dialog box (Figure 6-164) or the **Shutdown Log Search** dialog box opens (Figure 6-165).

*Figure 6-164. Event Log Search Dialog Box*

*Figure 6-165. Event Log Search Dialog Box*

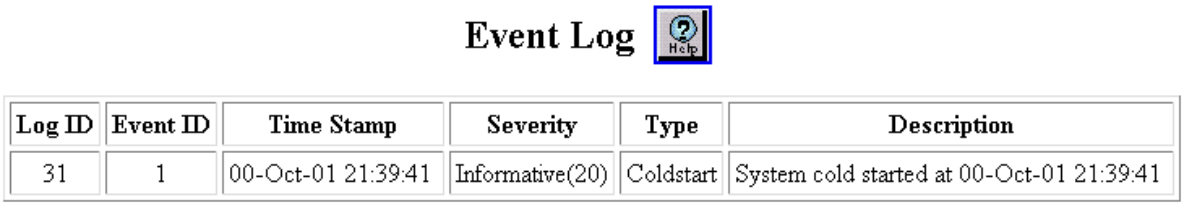
2. Click the **Severity Level** checkbox in the **Search By:** column on either dialog box.

3. Select the severity level to filter on a particular severity level for events from the **Severity Level** field pull-down menu from either dialog box.

4. Select an event to filter on a particular event type from the **Event Type** field pull-down menu from either dialog box. The event log entries open in the **Event Log** dialog box (Figure 6-166).

*** Note:** If you do not select a **Severity level** or **Event Type,** the entire Event/Shutdown log is displayed.

*Figure 6-166. Event Log Dialog Box*




5. Refer to Table 6-112 for a explanation **Event Log** dialog box parameters:

*Table 6-112. Event Log Window Parameters*

| Entry | Definition |
|---|---|
| **Log ID** | Displays the number of this event in the log FIFO (First In First Out). |
| **Event ID** | Displays an index that identifies the event class. |
| **Time Stamp** | Displays the date and time the event was recorded. |
| **Severity** | Displays the severity of the event. The possibilities are:<br>• Normal<br>• Informative<br>• Warning<br>• Alarm<br>• Error<br>• Fatal |
| **Type** | Displays a description of the event type (for example System start and Status Change). |
| **Description** | Displays a text string that describes the specific event with the date and time of the event.<br>**Note:** The time is displayed in yy/mm/dd sequence: |

6. Click...

   — **SEARCH** to view the event or shutdown logs from either dialog box.

   — **CANCEL** to restore previous settings.

   — **CLEAR EVENT LOG** to clear the event log settings.

   *** Note:** You can clear the event log by clicking Clear Event Log, If you have write-access. This option is not available if you do not have write-access.

### Using the CLI

To view the Event and Shutdown logs using the CLI, enter the following command from **Configuration** mode:

```
<configure># show logging <num-events|shutdown|CR>
```

*** Note:** Show logging CR will display the entire log.

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about these commands.

## Viewing Event Statistics

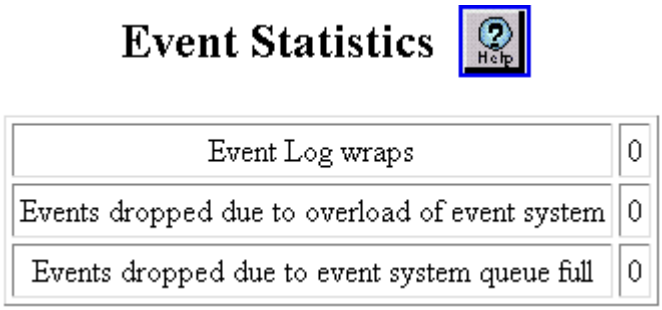
You can view event statistics using either the Web Agent or the CLI.

### Using the Web Agent

To view event statistics using the Web Agent:

1. Select **Statistics** from the **Events** group on the Web Agent window. The **Event Statistics** dialog box opens (Figure 6-167).

***Figure 6-167. Event Statistics Dialog Box***



2. Refer to the Table 6-113 for an explanation on the **Event Statistics** window parameters.

*Table 6-113. Event Statistics Window Parameters*

| Parameter | Definition |
|---|---|
| **Event Log wraps** | Displays the number of times the Event Log has wrapped. The Event Log may or may not wrap, depending on how many events have been sent to the Event Log and when it was last cleared. When the event log does wrap, the old events are discarded and replaced with the newest events. |
| **Events dropped due to overload of event system** | Displays the number of events that were dropped to prevent overloading. |
| **Events dropped due to event system queue full** | Displays the number of events that were dropped due to a full Event System queue. |

### Viewing Event Statistics Using the CLI

To view a specific number of event statistics using the CLI, enter the following command from **Configuration** mode:

```
<configure># show logging <num-events>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about these commands.

## Setting Log Size

You can set the log size using either the Web Agent or the CLI.

### Setting Log Size Using the Web Agent

To set the log size using the Web Agent:

1. Select **General Events** from the **Events** group on the Web Agent window. The **General Event Management** dialog box opens (Figure 6-162).

2. Select the number of entries you want to store in each of the switch event logs from the **Event Log** field pull-down menu.

3. Refer to Table 6-114 for an explanation of the **Event Log** and **Shutdown Log** parameters on the **General Event Management** dialog box:

*Table 6-114. Event Log and Shutdown Log Fields Parameters*

| Log | Purpose |
|---|---|
| **Event Log** | A detailed, ongoing record of syslog messages that are stored in the router's history table. This log is stored in memory and is erased if the system shuts down or reboots. |
| **Shutdown Log** | Contains a list of events that occurred before the last time the switch was shutdown. Because this log is stored in nonvolatile memory, it is preserved during a switch reboot or shutdown. It is designed to help you analyze the events that occurred immediately prior to a switch shutdown or reset. |

4. Refer to Table 6-115 for an explanation of the items listed in the **Class** column on the **General Event Management** dialog box:

*Table 6-115. Class Column Items*

| Class | Determines whether or not the switch sends a notification... |
|---|---|
| **Start** | Upon System start. |
| **System** | For system events. |
| **Configuration** | For each configuration change (for example, enabling and disabling ports). |
| **Temperature Status** | For Temperature status changes. Temperature status messages could precede a switch shutdown, and are often critical. |
| **Resource** | Upon a change in system resources. |
| **Fan Status** | Of fan status. Fan failures will eventually lead to overheating the system. The Fan Status message provides a good early warning for a failure that could eventually cause the switch to shut down. |
| **Service Port Status/ User Port Status** | Of Port status changes for service and user ports. Set a port as either service port/user port from the port configuration page. The purpose of this feature is to allow you to use different notification level for critical (service ports), if desired. |
| **Authentication Failure** | When the switch detects an authentication failure. This is a security-related feature used to detect unauthorized SNMP activity. |

*Table 6-115. Class Column Items continued*

| Class | Determines whether or not the switch sends a notification... |
|---|---|
| **Bridge Status** | Of changes in bridge status. |
| **Switch Fabric** | Of failures in the switch fabric. These are critical failures and should be monitored closely. |
| **OSPF** | For OSPF events if OSPF protocol event logging is enabled. |
| **RIP** | For RIP events if RIP protocol event logging is enabled. |
| **LDAP** | For LDAP events if LDAP protocol event logging is enabled. |
| **AppleTalk** | For AppleTalk events if AppleTalk protocol event logging is enabled. |
| **Power Status** | Addition or Removal of a Power Supply |
| **Redundant CPU** | When a redundant Supervisor is used. Message will indicate changes in Active and Standby status of the CPU |
| **DVMRP** | For DVMRP events, if DVMRP event logging is enabled. |
| **CLI** | For CLI events, if CLI event logging is enabled. |
| **SNMP** | For SNMP events, if SNMP protocol event logging is enabled. |
| **Unknown MAC Received** | If an unknown MAC address is received. |
| **VRRP** | For VRRP events, if VRRP protocol event logging is enabled. |

5. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Using the CLI

To set log size using the CLI, enter the following command from **Configuration** mode:

```
<configure>#set logging history size <128, 512,
1024, 2048>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about these commands.

# Configuring Event Notification

You can Configure event notification using either the Web Agent or the CLI.

## Using the Web Agent

To Configure Event Notification from the Web Agent:

1. Select **General Events** from the **Events** group on the Web Agent window. The **General Event Manager** dialog box opens (Figure 6-162).
2. Click the check box in the **ID Field** of the event you wish to log.
3. Click on the checkbox next to the **log** in the **Action column** for every event you wish to log.
4. Click **APPLY** to configure or **CANCEL** to ignore.

## Using the CLI

To configure Event Notification using the CLI, enter the following command from **Configuration** mode:

```
<configure># logging history <event>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about these commands.

# 18 Monitoring and Configuring the Forwarding Cache

## Overview

The information and procedures provided in this chapter pertain to layer 3 module configuration only:

- Configuring the Fowarding Cache
- Displaying Frame Fowarding Statistics
- Displaying and Searching the L3 Forwarding Cache for an Entry
- Displaying the Forwarding Cache

## Configuring the Fowarding Cache

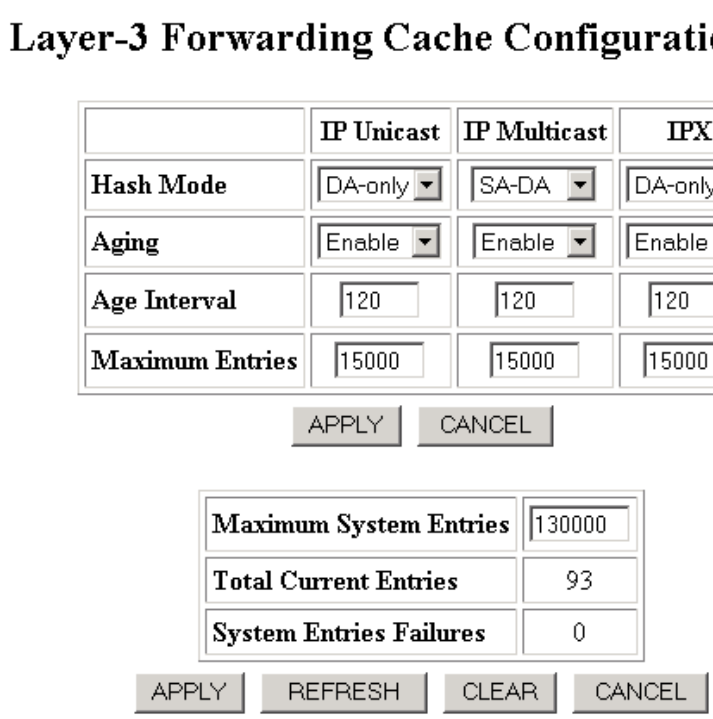
The forwarding cache enables you to configure the multilayer media module's forwarding tables. You can configure the forwarding cache using the Web Agent or the CLI.

### Using the Web Agent

To configure the forwarding cache using the Web Agent:

1. Select **Cache Configuration** from the **Routing > L3 Forwarding Cache** group on the Web Agent window. The **Layer 3 Forwarding Cache Configuration** dialog box opens (Figure 18-1).

*Figure 6-168. Layer-3 Forwarding Cache Configuration Dialog Box*




2. Configure the Layer 3 Forwarding Cache configuration parameters. Refer to Table 6-116 for an explanation of the **Layer-3 Forwarding Cache Configuration** dialog box parameters for tree configuration:

*Table 6-116. Layer-3 Forwarding Cache Configuration Dialog Box Parameters for Tree Configuration*

| Tree Configuration | | |
|---|---|---|
| **Field...** | **For the protocol...** | **Allows you to...** |
| **Hash Mode** | IP Unicast (IPU)<br>IP Multicast (IPM)<br>IPX | Configure the table hash lookup mode for the IP unicast, IP multicast and IPX protocols. The options are:<br>• **DA-only** - Forwarding entries input to the forwarding table are limited to using protocol destination address only.<br>• **SA-DA** - Forwarding entries input to the forwarding table are limited to using destination and source address only. |
| **Aging** | IP Unicast<br>IP Multicast<br>IPX | Configure the IP unicast, IP multicast, or IPX protocols forwarding table entry aging status as either **Enable (default)** or **Disable**. |
| **Age Interval** | IP Unicast<br>IP Multicast<br>IPX | The IP unicast, IP multicast, or IPX protocols forwarding table entry aging period (in seconds). The valid range is **20-360** seconds. The default value is **120** seconds. |
| **Maximum Entries** | IP Unicast<br>IP Multicast<br>IPX | The number of active entries in the IP unicast, IP multicast, or IPX protocol forwarding table. This is the maximum number of active entries per fabric port. Additional flows are forwarded by the supervisor module. The default value is **15000**. |

3. Click:
   - **APPLY** to save your changes
   - **CANCEL** to restore previous settings
   - **REFRESH** to update your system configuration
   - **CLEAR** to reset all configuration parameters to zero.

## Using the CLI

To configure the forwarding cache using the CLI, enter the following command from Configure mode:

```
<configure># ip multicast route-cache <options>
<configure># ip unicast route-cache <options>
```

```
<configure># ipx route-cache <options>
```

*** Note:** There is no CLI command to clear the L3 FE cache.

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about these commands.

# Monitoring the Forwarding Cache Statistics

Monitoring the forwarding cache statistics includes:

- Displaying Frame Fowarding Statistics
- Displaying and Searching the L3 Forwarding Cache for an Entry

## Displaying Frame Fowarding Statistics

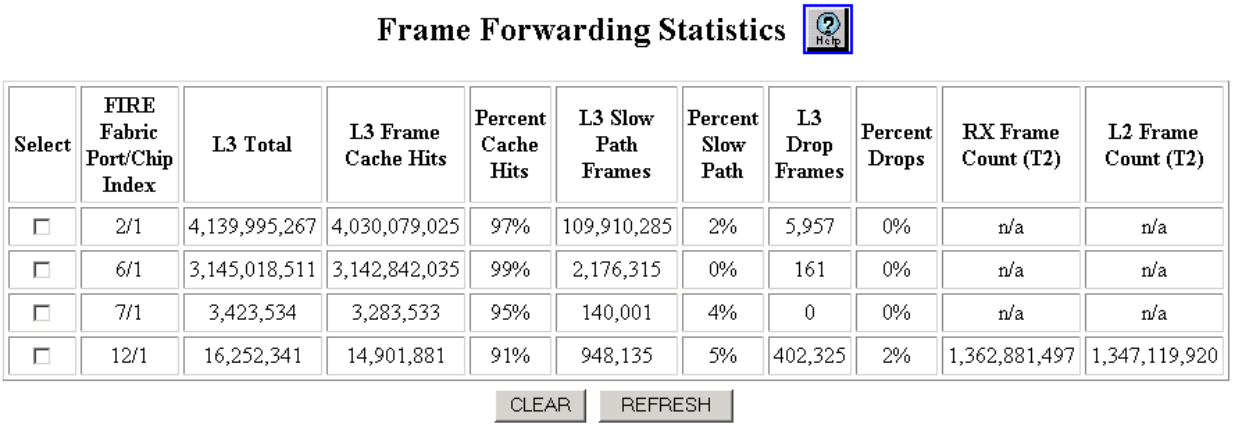
The frame forwarding statistics indicate the performance of each of the multilayer media modules in respect to layer 3 routing and forwarding. You can display the frame forwarding statistics from either the Web Agent or the CLI.

### Using the Web Agent

To display the frame forwarding statistics using the Web Agent:

1. Select **Forwarding Statistics** from the **Routing > L3 Forwarding Cache** group on the Web Agent window. The **Frame Forwarding Statistics** dialog box opens (Figure 6-169).

*Figure 6-169. Frame Forwarding Statistics Dialog Box*


Frame Forwarding Statistics
Help
Select
FIRE Fabric Port/Chip Index
L3 Total
L3 Frame Cache Hits
Percent Cache Hits
L3 Slow Path Frames
Percent Slow Path
L3 Drop Frames
Percent Drops
RX Frame Count (T2)
L2 Frame Count (T2)
2/1 4,139,995,267 4,030,079,025 97% 109,910,285 2% 5,957 0% n/a n/a
6/1 3,145,018,511 3,142,842,035 99% 2,176,315 0% 161 0% n/a n/a
7/1 3,423,534 3,283,533 95% 140,001 4% 0 0% n/a n/a
12/1 16,252,341 14,901,881 91% 948,135 5% 402,325 2% 1,362,881,497 1,347,119,920
CLEAR
REFRESH

2. Refer to Table 6-117 for an explanation for the Frame Forwarding Statistics dialog box parameters

*Table 6-117. Frame Forwarding Statistics Dialog Box Parameters*

| Parameter | Defines the... |
|---|---|
| **FIRE Fabric Port/Chip Index** | Fabric port associated with the layer 3 module. The P550/P580 switch has 13 fabric ports: the P880/P882 switch has 33 fabric ports. The supervisor module slot uses one fabric port: the media module slots each use two fabric ports. The supervisor module slot uses fabric port 1, the first media module slot uses fabric ports 2 and 3, and so on. |
| **L3 Total (T2)** | Total number of frames received on the fabric port. |
| **L3 Frame Cache Hits** | Number of packets received on the fabric port that were successfully matched against existing forwarding entries in the layer 3 (L3) address cache. |
| **Percent Cache Hits** | Total percentage of successful matches between packets received on a fabric port and the percent of those packets that matched the L3 address cache entries. |
| **L3 Slow Path Frames** | Number of frames received on a fabric port that were *not* successfully matched against existing forwarding entries in the layer 3 (L3) address cache. Subsequently, these frames were forwarded to the supervisor module (slow path). All frames sent to the supervisor module are routed in software. |
| **Percent Slow Path** | Total percentage of unsuccessful matches between packets received on a fabric port and the percent of those packets that did not match the layer 3 address cache entries. |

*Table 6-117. Frame Forwarding Statistics Dialog Box*

| Parameter | Defines the... |
|---|---|
| **L3 Drop Frames** | Number of layer 3 frames that were dropped. For example: They did not match the layer 3 address cache entries. |
| **Percent Drops** | Total percent of layer 3 frames dropped. |
| **RX Frame Count (T2)** | Total number of frames received on a fabric port. |
| **L2 Frame Count (T2)** | Number of layer 2 frames received on a fabric port that were forwarded on to an associated VLAN. |

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about these commands.

# Displaying and Searching the L3 Forwarding Cache for an Entry

## Using the Web Agent

You can display and search the Layer 3 Forwarding Cache for an entry using the web agent, To display the contents of the L3 forwarding Cache, you can use the search function to display:

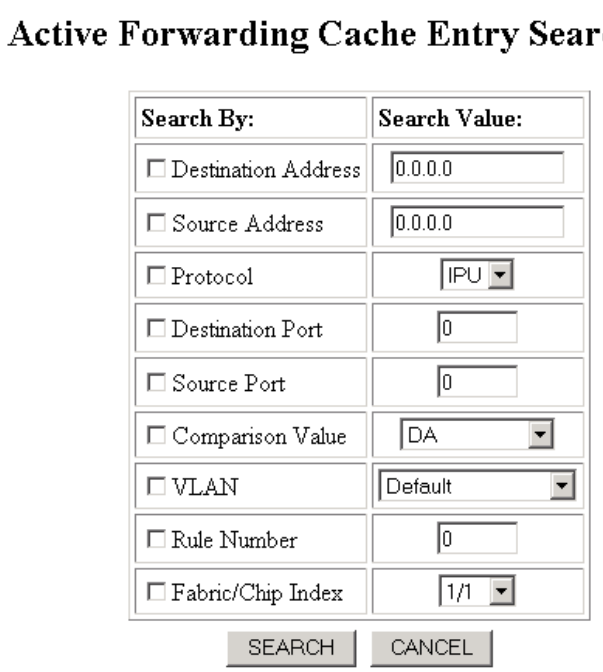
- only the selected options,
- or all options by not selecting any options and clicking on the search button.

*** Note:** Layer 3 Active Forwarding Cache entry Search is available with the Web Agent only, no CLI version.

To search the L3 address cache using the Web Agent:

1. Select **Entry Search** from the **Routing > L3 Forwarding Cache** group on the Web Agent window. The **Active Forwarding Cache Entry Search** dialog box opens (Figure 6-170).

*Figure 6-170. Active Forwarding Cache Entry Search Dialog Box*




Select the search criteria that you want to use to find more specific information on available routes from the Search By column.

For example, if you want to find all entries in the Forwarding Cache by a VLAN, you would select the VLAN from the **Search By** column, and select the appropriate VLAN from the pull-down menu.Figure 18-4 is the actual display results from a Forwarding Cache search done by a VLAN.
Refer to Table 6-118 for an explanation of the **Route Cache Entry Search** dialog box parameters:

*Table 6-118. L3 Forwarding Cache Entry Search Dialog Box Parameters*

| Parameter | Allows you to search for all entries... |
|---|---|
| **Destination Address** | Within the routing cache that match the specified destination address (IP address), or IPX network number |
| **Source Address** | Within the routing cache that match the specified source address (IP address), or IPX network number |
| **Protocol** | By protocol identifier. By default, this field is 0 for IP. |

*Table 6-118. L3 Forwarding Cache Entry Search Dialog Box Parameters continued*

| Parameter | Allows you to search for all entries... |
|---|---|
| **Destination Port** | Within the routing cache that match the specified destination port (IPU, IPM, IPX). |
| **Source Port** | Within the routing cache that match the specified source port (IPU, IPM, IPX). |
| **Comparison Value** | Within the routing cache that match the specified comparison value (TCP/UDP). Values include:<br>• **DA** - Destination address<br>• **DASA** - Destination and source address<br>• **DAPROT** - Destination address and protocol<br>• **DADP** - Destination address and destination port number<br>• **DASAPROT** - Destination and source address and protocol<br>• **DASADPSP** - Destination and source address, and the corresponding destination and source port numbers |
| **VLAN** | Within the routing cache that match the VLANs listed in the pull-down menu. |
| **Rule Number** | Within the routing cache that matches the specified rule number associated with an access list. |
| **Fabric/Chip Index** | Match the Forwarding Chip that is associated with the fabric port ID. |

*Figure 6-171. Forwarding Cache Search by VLAN*

Active Forwarding Cache


| Fabric/Chip Index | Tree | Access Rule | DA | SA | DP | SP | Comp | TTL | Age | Filter | Destination VLAN | Source VLAN | Mac Address | Use | Priority | Format |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2/1 | IP_UNI | None | 10.0.1.22 | 0.0.0.0 | 0 | 0 | DA | 0 | 7 | No | vlan10 | n/a | 02:e0:3b:e9:28:09 | 0 | 1 | Eth2 |
| 4/1 | IP_UNI | None | 10.0.1.22 | 0.0.0.0 | 0 | 0 | DA | 0 | 7 | No | vlan10 | n/a | 02:e0:3b:e9:28:09 | 0 | 1 | Eth2 |
| 4/1 | IP_MUL | None | 239.255.0.1 | 10.0.4.8 | 0 | 0 | DA | 0 | 0 | No | vlan10 | vlan5 | Derived from DA | 1 | 1 | Eth2 |
| 6/1 | IP_UNI | None | 10.0.1.22 | 0.0.0.0 | 0 | 0 | DA | 0 | 7 | No | vlan10 | n/a | 02:e0:3b:e9:28:09 | 0 | 1 | Eth2 |
| 7/1 | IP_UNI | None | 10.0.1.22 | 0.0.0.0 | 0 | 0 | DA | 0 | 7 | No | vlan10 | n/a | 02:e0:3b:e9:28:09 | 0 | 1 | Eth2 |

### Using the CLI

To display the L3 Forwarding Cache cache using the CLI, enter one of the following commands from **configure** mode for the specific routing cache:

```
<configure># show ip unicast cache

<configure># show ip multicast cache

<configure># show ipx cache
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about these commands.

## Displaying the Forwarding Cache

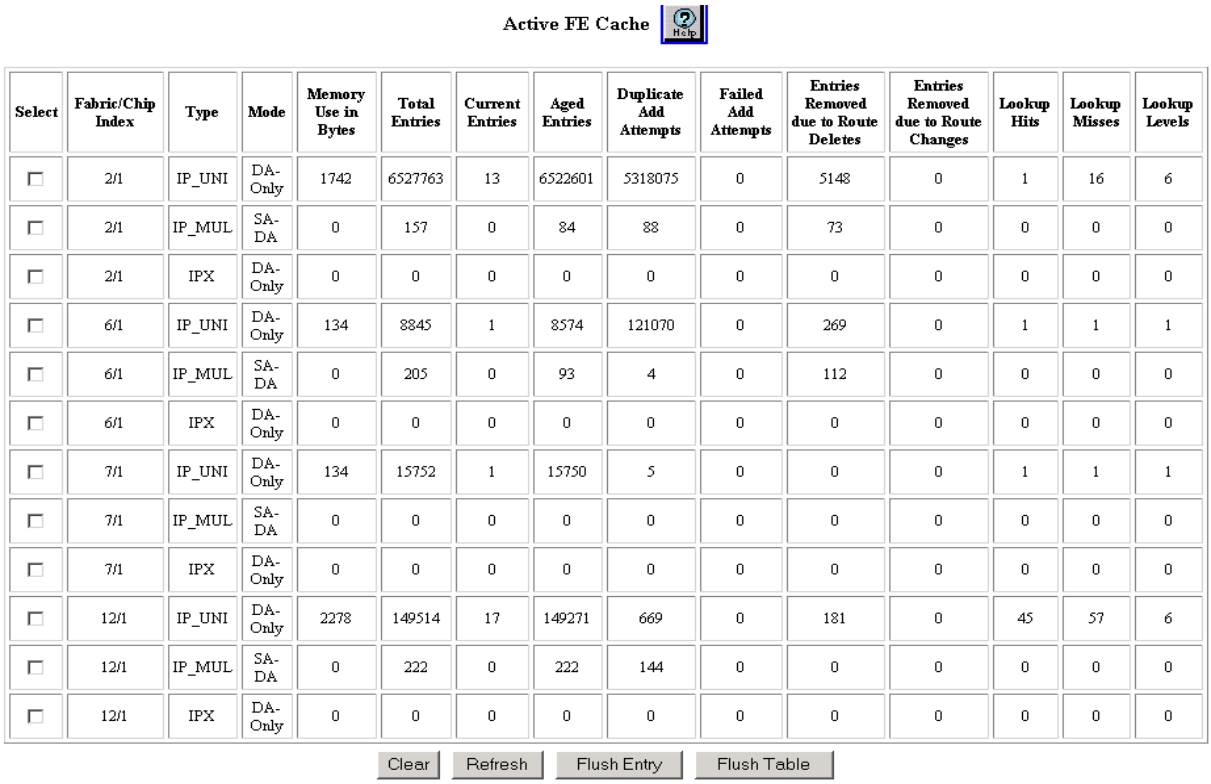
You can display the Forwarding cache information using either the Web Agent or the CLI.

### Using the Web Agent

To display the forwarding cache information using the Web Agent:

1. Select Cache Contents from the Routing > L3 Forwarding Cache group on the Web Agent window.
2. The FE Cache dialog box opens (Figure 18-5).

*Figure 6-172. Active FE Cache Dialog Box*




| Select | Fabric/Chip Index | Type | Mode | Memory Use in Bytes | Total Entries | Current Entries | Aged Entries | Duplicate Add Attempts | Failed Add Attempts | Entries Removed due to Route Deletes | Entries Removed due to Route Changes | Lookup Hits | Lookup Misses | Lookup Levels |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 2/1 | IP_UNI | DA-Only | 1742 | 6527763 | 13 | 6522601 | 5318075 | 0 | 5148 | 0 | 1 | 16 | 6 |
| ☐ | 2/1 | IP_MUL | SA-DA | 0 | 157 | 0 | 84 | 88 | 0 | 73 | 0 | 0 | 0 | 0 |
| ☐ | 2/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 6/1 | IP_UNI | DA-Only | 134 | 8845 | 1 | 8574 | 121070 | 0 | 269 | 0 | 1 | 1 | 1 |
| ☐ | 6/1 | IP_MUL | SA-DA | 0 | 205 | 0 | 93 | 4 | 0 | 112 | 0 | 0 | 0 | 0 |
| ☐ | 6/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 7/1 | IP_UNI | DA-Only | 134 | 15752 | 1 | 15750 | 5 | 0 | 0 | 0 | 1 | 1 | 1 |
| ☐ | 7/1 | IP_MUL | SA-DA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 7/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 12/1 | IP_UNI | DA-Only | 2278 | 149514 | 17 | 149271 | 669 | 0 | 181 | 0 | 45 | 57 | 6 |
| ☐ | 12/1 | IP_MUL | SA-DA | 0 | 222 | 0 | 222 | 144 | 0 | 0 | 0 | 0 | 0 | 0 |
| ☐ | 12/1 | IPX | DA-Only | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**3.** To modify your FE Cache table, do one of the following:

— Select the entry and click **Flush Entry** to delete one or more entries

— Click **Flush Table** to clear the entire table

*** Note:** Flushing the table will disrupt traffic flow and clear all Forwarding Entries, and all flows must be relearned.

— Click **REFRESH** to refresh the contents of the table

— Click **Clear** to remove the statistics only (the entry in the table remains).

4. Refer to Table 6-119 for an explanation of the **FE Cache** dialog box fields:

*Table 6-119. FE Cache Dialog Box Fields*

| Parameter | Defines... |
|---|---|
| **Fabric/Chip Index** | The Packet Routing Engine in question. |
| **Type** | The type of packet (for example, IP unicast, IP multicast). |
| **Mode** | The table mode which includes:<br>• DA-Only<br>• SA & DA<br>The table mode indicates what values are used in a comparison to determine whether or not a packet is forwarded. |
| **Memory Use in Bytes** | Memory used by each entry. |
| **Total Entries** | The number of cumulative entries since the last time the statistics were cleared. |
| **Current Entries** | The number of active entries. |
| **Aged Entries** | The number of entries aged out. |
| **Duplicate Add Attempts** | The number of attempts at adding the same slow path entries. |
| **Failed Add Attempts** | The number of failed attempts at adding a forwarding entry. |
| **Entries Removed Due to Route Deletes** | The number of entries removed because of route deletions. |
| **Entries Removed Due to Route Changes** | The number of entries removed because of route changes. |
| **Lookup Hits** | The number of incoming packets that was found in the cache. |
| **Lookup Misses** | The number of incoming packets that was not found in the cache. |
| **Lookup Levels** | Cache depth. |

# 19 Analyzing Network Performance By Using RMON and Ethernet Statistics

## Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations:

- Viewing Network Statistics
- Setting Up Port Mirroring
- Enabling MAC Address Lock and Traps for Unknown Source Addresses

## Viewing Network Statistics

You can view a variety of statistics from the switch interface that allows you to monitor network performance and troubleshoot network problems.

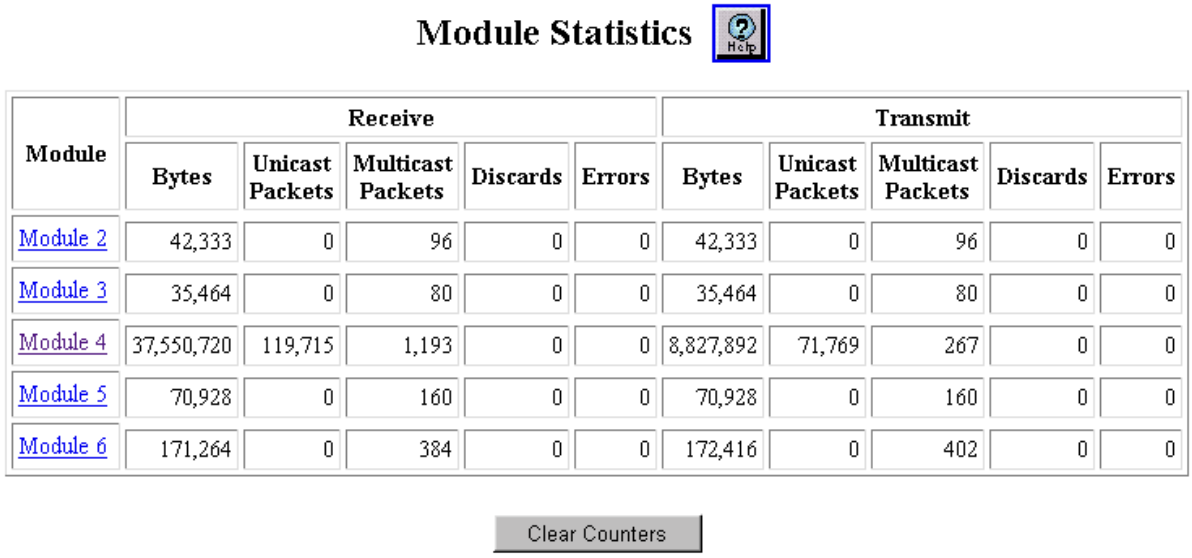
You can view statistics using either the Web Agent or the CLI.

### Web Agent Procedure

To view network statistics by using the Web Agent:

1. Select **Statistics** from the **Modules & Ports** group on the Web Agent window. The **Module Statistics** Web page opens (Figure 6-173).

*Figure 6-173. Module Statistics Web page*



Module Statistics

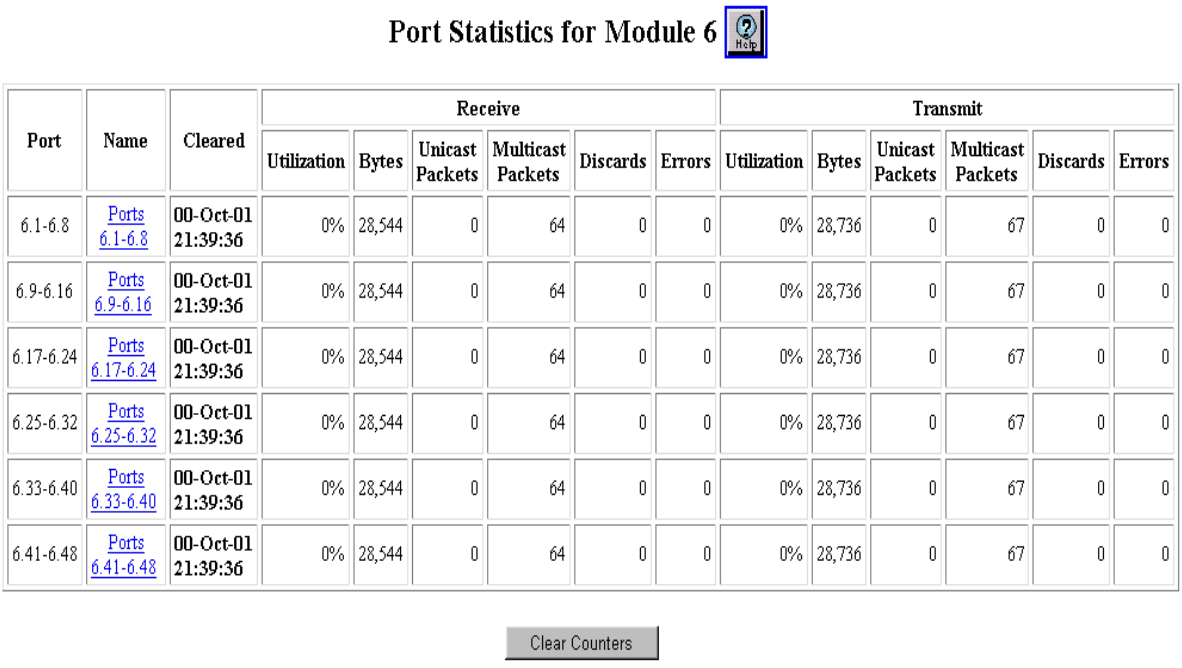
| Module | Receive | | | | | Transmit | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Bytes | Unicast Packets | Multicast Packets | Discards | Errors | Bytes | Unicast Packets | Multicast Packets | Discards | Errors |
| Module 2 | 42,333 | 0 | 96 | 0 | 0 | 42,333 | 0 | 96 | 0 | 0 |
| Module 3 | 35,464 | 0 | 80 | 0 | 0 | 35,464 | 0 | 80 | 0 | 0 |
| Module 4 | 37,550,720 | 119,715 | 1,193 | 0 | 0 | 8,827,892 | 71,769 | 267 | 0 | 0 |
| Module 5 | 70,928 | 0 | 160 | 0 | 0 | 70,928 | 0 | 160 | 0 | 0 |
| Module 6 | 171,264 | 0 | 384 | 0 | 0 | 172,416 | 0 | 402 | 0 | 0 |

Clear Counters

2. Select **Clear Counters** to get a fresh view of the statistics being gathered. This resets all of the counters to zero, so that you can track the counters from a specific point forward.

3. Select a module from the **Module** column to view statistics for that specific module. The **Port Statistics** Web page opens (Figure 19-2).

*Figure 6-174. Port Statistics Web page*



Port Statistics for Module 6

| Port | Name | Cleared | Receive | | | | | | Transmit | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Utilization | Bytes | Unicast Packets | Multicast Packets | Discards | Errors | Utilization | Bytes | Unicast Packets | Multicast Packets | Discards | Errors |
| 6.1-6.8 | Ports 6.1-6.8 | 00-Oct-01 21:39:36 | 0% | 28,544 | 0 | 64 | 0 | 0 | 0% | 28,736 | 0 | 67 | 0 | 0 |
| 6.9-6.16 | Ports 6.9-6.16 | 00-Oct-01 21:39:36 | 0% | 28,544 | 0 | 64 | 0 | 0 | 0% | 28,736 | 0 | 67 | 0 | 0 |
| 6.17-6.24 | Ports 6.17-6.24 | 00-Oct-01 21:39:36 | 0% | 28,544 | 0 | 64 | 0 | 0 | 0% | 28,736 | 0 | 67 | 0 | 0 |
| 6.25-6.32 | Ports 6.25-6.32 | 00-Oct-01 21:39:36 | 0% | 28,544 | 0 | 64 | 0 | 0 | 0% | 28,736 | 0 | 67 | 0 | 0 |
| 6.33-6.40 | Ports 6.33-6.40 | 00-Oct-01 21:39:36 | 0% | 28,544 | 0 | 64 | 0 | 0 | 0% | 28,736 | 0 | 67 | 0 | 0 |
| 6.41-6.48 | Ports 6.41-6.48 | 00-Oct-01 21:39:36 | 0% | 28,544 | 0 | 64 | 0 | 0 | 0% | 28,736 | 0 | 67 | 0 | 0 |

Clear Counters

4. Click **Clear Counters** to get a fresh view of the statistics being gathered. This resets all of the counters to zero so that you can track the counters from a particular point forward.

5. Select a port from the **Name** column to view statistics for that specific port. The **Ethernet Interface Statistics** Web page opens (Figure 19-3).

***Figure 6-175. Ethernet Interface Statistics Web page***

**Available History Links (mm:ss) :**

0:30 sample

30:0 sample

**Ethernet Interface Statistics**

| Statistic | Total | Receive | Transmit |
|---|---|---|---|
| Utilization | 0% | 0% | 0% |
| Bytes | 57,280 | 28,544 | 28,736 |
| Unicast Packets | 0 | 0 | 0 |
| Multicast Packets | 131 | 64 | 67 |
| Discards | 0 | 0 | 0 |
| Errors | 0 | 0 | 0 |
| Pause Frames | 0 | 0 | 0 |

**Error Detail**

6. Select either **0:30 sample** (30 second sample) or **30:0 sample** (30 minute sample) from the **Available History Links** field. The **Ethernet Interface Statistics** Web page opens with the sample you selected.

7. Refer to Table 6-120 for an explanation of the **Ethernet Interface Statistics** Web page fields:

***Table 6-120. Ethernet Interface Statistics Web Page Fields***

| Statistic | Indicates | Actions |
|---|---|---|
| **Sample** | The sample number. | N/A |
| **Interval Start** | The date and time this log entry was made. | N/A |
| **Utilization** | Percentage of utilization. | The percentage of available bandwidth used by traffic. |
| **Bytes** | Raw number of octets received at the interface. Provides some indication of the amount of network bandwidth being used. | A sharp increase could indicate a need to reconfigure the network. |
| **Packets** | Counts the raw number of readable Ethernet packets of legal length received at the interface. | A sharp increase could indicate a need to reconfigure the network. (However, octets are a better indication of bandwidth utilization.) |
| **Broadcasts** | Broadcast packets are a normal part of network operation. For example, IP networks use broadcasts as part of Address Resolution Protocol (ARP) to resolve network addresses. | Uses monitoring to recognize oncoming broadcast storms. Broadcast storms occur when stations are creating traffic that generates more traffic.<br>**Possible cause:** Broadcasts cause every host on a network segment to process the packet.<br>Possible actions:<br>• To prevent broadcast storms, use VLANs to limit the area of the network that each broadcast packet affects. In general, each VLAN creates a separate broadcast domain. More VLANs mean less proliferation of broadcast packets.<br>• Monitor the broadcast rate of your network during normal operation.<br>• Establish a baseline.<br>• Use Rate Limiting to reduce broadcasts. |
| | | ***1 of 4*** |

*Table 6-120. Ethernet Interface Statistics Web Page Fields*

| Statistic | Indicates | Actions |
|---|---|---|
| **Multicasts** | Normal during network operation. For example, multicast packets are to send target video streams to selected stations on the network, and are part of the operation of the Spanning Tree Protocol. | **Possible causes:**<br>• Too many multicast frames can consume valuable network bandwidth.<br>**Possible actions:**<br>• Using Intelligent Multicasting can significantly reduce multicast traffic on individual ports.<br>• Segmenting the network into smaller VLANs and routing between them can also help control proliferation of multicasts. |
| **CRC (Cyclic Redundancy Check) or Alignment Errors** | Counts of the number of times that the number of bits in a frame cannot be divided by 8 (that is, cannot be broken into legal octets), and that contain a Frame Check Sequence validation error. Typically caused by turning equipment on or off, and by noise on twisted pair segments. These errors can also result from configuring a network that does not comply with 802.3 standards. In a standards-compliant Ethernet network, CRC or alignment errors represent transit and receive bit errors.<br>The Ethernet standard allows 1 in $10^8$ bit error rate, but you should expect performance to be less than 1 in $10^{12}$ packets. Rates in excess of one error per one thousand packets indicate a serious problem. | **Possible causes**:<br>• Defect at the transmitting station.<br>• Turning equipment on or off. This should cause only a few errors.<br>• Damaged cables.<br>• Interference on network cabling.<br>**Possible action**s (respectively):<br>• Use port error statistics to isolate the problem. Check the transceiver or adapter card connected to the port where the problem seems to originate. Also check the cable and cable connections for damage.<br>• Normal operation, no action required.<br>• Check cables for damage.<br>• Inspect cable runs to see if they are too close to noisy devices, and check for problems with network devices. |
| | | ***2 of 4*** |

*Table 6-120. Ethernet Interface Statistics Web Page Fields*

| Statistic | Indicates | Actions |
|---|---|---|
| **Undersized Packets** | Count of packets with a valid CRC that violate the minimum Ethernet packet size.<br>These malformed packets are most often the result of software errors. | **Possible cause:** Device or application creating non-compliant packets.<br>**Possible action:** Use a network analyzer to identify the which transceiver which is at the source of the problem. Replace the transceiver, network adapter, or station. |
| **Oversized Packets** | Count of packets with a valid CRC that violate the maximum Ethernet packet size.<br>These malformed packets are most often the result of software errors. | **Possible cause:** Device or application creating non-compliant packets.<br>**Possible action:** Use a network analyzer to identify the transceiver which at the source of the problem. Replace transceiver, network adapter, or station. |
| **Fragments** | Fragments or runts result from normal collision activity in Ethernet networks. A runt packet is an incomplete packet that is long enough to be detected by an Ethernet interface. | **Possible causes**:<br>• Interference on network cabling.<br>• A Transceiver attached to the Repeater is generating Signal Quality Errors (SQE).<br>**Possible actions (respectively)**:<br>• Inspect cable runs to see if they are too close to noisy devices, and check for problems with network devices.<br>• Disable SQE on the Transceiver. |
| | | ***3 of 4*** |

*Table 6-120. Ethernet Interface Statistics Web Page Fields*

| Statistic | Indicates | Actions |
|---|---|---|
| **Jabbers** | Jabbers indicate that devices on the networks are sending improper electrical signals. Because Ethernet uses electrical signalling to determine whether or not it is okay to transmit, a jabber condition can halt all traffic on a segment. | **Possible causes**:<br>• Bad network interface card<br>• Repeater network with looped traffic<br>**Possible actions (respectively):**<br>• Replace the network interface card.<br>• Rewire network to remove the loop. |
| **Collisions (half-duplex links only)** | Counts number of times that packets have collided on the network. Collisions increase as network use of shared segments increases. Therefore, if the collision rate increases without an increase of network use, it might indicate a problem. Guidelines for appropriate collision rates are:<br>• 10 percent: Normal collision rate for shared Ethernet segment.<br>• 30 percent: Collisions begin to interfere with performance.<br>• 70 percent: Practical limit for network to remain functioning.<br>A full-duplex link should not show collision activity. Collisions are rare in a switched network, unless your switched segments attach to multiple ends stations (a legal configuration option). | **Possible causes**:<br>• Busy network<br>• Broken adapter (not listening before broadcasting)<br>• Network loop<br>**Possible actions (respectively)**:<br>• If you have multiple stations on a switch segment, reconfigure network into segments with fewer stations.<br>• Isolate each adapter to see if the problem ceases.<br>• Activate spanning tree to resolve loops automatically.<br>• Ensure that there are no connections to the same station where both connections are simultaneously active. |
| | | ***4 of 4*** |

## Using the CLI

To view network statistics using the CLI, enter the following command in **Privileged** mode:

```
<configure># show ethernet counters <cr|mod-
num|mod-swport-spec>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

# Setting Up Port Mirroring

Configuring an RMON mirror port allows you to mirror traffic from a port or set of ports to a specific mirror port, where you can attach a sniffer or RMON probe. The switch supports a single mirror port and a single source port for each switch fabric port. For example, 20-port Fast Ethernet cards have two fabric ports (one for ports 1 through 10, one for ports 11 through 20). You can set up a single source port and a single mirror port for each set of ports associated with a fabric port. You can also choose to mirror all traffic from a particular fabric port to the mirror port, or set up multiple source ports to mirror traffic to a single mirror port.

Packets addressed to the CPU, such as pings, are duplicated out of the mirror port. Tagged packets that are sent into a source port with a VLAN ID to which the source port is not bound, are not transmitted out the mirror port. VLAN tag information is not propagated to the mirror port.

*** Note:** To prevent unnecessary traffic flooding on a mirror port, put the mirror port on the same VLAN as the source port.

Two port mirroring features are available for the Avaya Multiservice switches: Fabric mode 1 port mirroring and Fabric mode 2 port mirroring. The switch must be in Fabric mode 2 to perform Fabric mode 2 port mirroring.

Fabric mode 1 port mirroring works with 50-series modules. Fabric mode 2 port mirroring works with 80-series modules.

*** Note:** If you use port mirroring, the **Frame Tags** field on the Switch Port Configuration Web page for the port must be set to **Use** (default).

# Setting Up a Port Mirror on a Switch in Fabric Mode 1

You can set up a port mirror on a switch in Fabric Mode 1 by using either the Web Agent, the CLI, or SNMP. Fabric mode 1 port mirroring works with 50-series modules.

*** Notes:** Do not use a router port as a piggyback port.

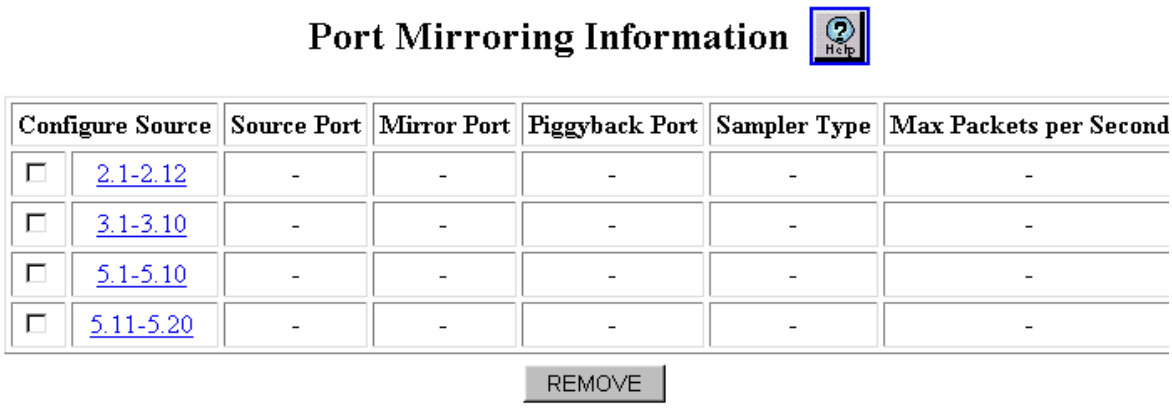
Do not set port mirroring on disabled ports.

You must establish a link to a mirror port before you setup a port mirror with a piggyback port. Otherwise, the port mirror will not work.

To set up a port mirror on a switch in Fabric mode 1 by using the Web Agent:

1. Select **Sampling** from the **Port Mirroring** group on the Web Agent window. The **Port Mirroring Information** Web page opens (Figure 6-176).

***Figure 6-176. Port Mirroring Information Web Page***




2. Refer to Table 2 for an explanation of the fields on the Port Mirroring Information Web page.

***Table 6-121. Port Mirroring Information Web Page Parameters***

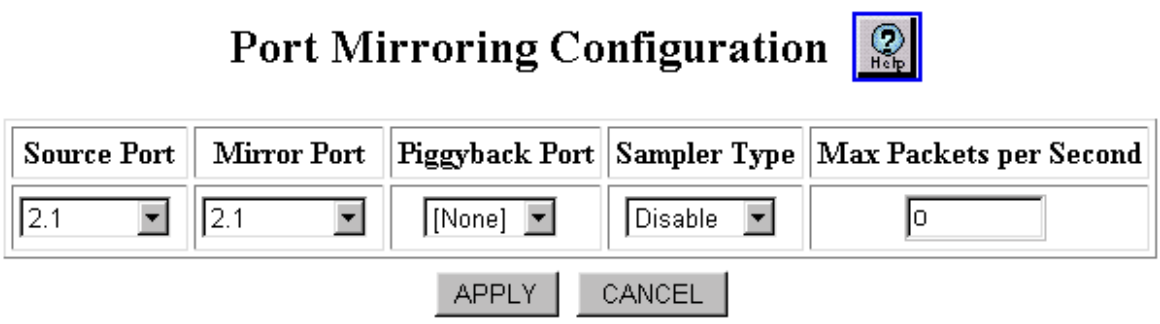
| Parameter | Definition |
|---|---|
| **Configure Source** | Select the configuration source port. Provides a link to the Port Mirroring Configuration Web page. |
| **Source Port** | Displays the port under investigation. |
| | ***1 of 2*** |

*Table 6-121. Port Mirroring Information Web Page Parameters*

| Parameter | Definition |
|---|---|
| **Mirror Port** | Displays the port that transmits mirrored data. |
| **Piggyback Port** | Displays the name of the port that is used for bi-directional port mirroring. When used as a mirror port, it is unavailable for other uses.<br>**Note:** 80 series modules do not support piggyback ports. |
| **Sampler Type** | Displays the speed of sampling that is performed for source port traffic. |
| **Max Packets per Second** | Displays the maximum number of packets per second that are served by the mirror port. |
| | *2 of 2* |

3. Select a source port for traffic from the **Configure Source** column. The **Port Mirroring Configuration** Web page opens (Figure 6-177).

*Figure 6-177. Port Mirroring Configuration Web page*



4. Refer to Table 6-122 for an explanation of the fields on the **Port Mirroring Configuration** Web page.

***Table 6-122. Port Mirroring Configuration Web Page Parameters***

| Parameter | Definition |
|---|---|
| **Source Port(s)** | List of available selections. You can select a particular source port associated with the selected fabric port. You can also select all ports.<br>**Note:** To mirror inbound traffic only, select a source port and a mirror port, not a piggyback port. |
| **Mirror Port** | Displays the port from which you want to send the traffic. This port can be on another module in the switch. Once a specific port associated with a fabric port has been designated a mirror port, other ports associated with that fabric port no longer appear on the selection list.<br>**Note:** The source port and the mirror port must be different physical ports. |
| | ***1 of 3*** |

*Table 6-122. Port Mirroring Configuration Web Page Parameters*

| Parameter | Definition |
|---|---|
| **Piggyback Port** | Port used to enable bi-directional port mirroring. If no piggyback port is specified, only received traffic from the source port will go to the mirror port. The piggyback port should have the same bandwidth as the source port. Only one port per fabric can be used as a piggyback port. Sampling rates have no effect on transmitted information.<br>**Considerations:**<br>• You cannot use a port that has been designated as a piggyback port.<br>• Once a port has been designated as a piggyback port, the link light is turned on, even if there is no connection on the selected port.<br>• The piggyback port is displayed in place of the source port in the VLAN menu.<br>• If the source and piggyback ports are at a higher bandwidth than the mirror port's bandwidth, the traffic on the source port may exceed the bandwidth that the mirror port can handle.<br>• The piggyback port will always show that it is using multi-layer tagging.<br>• A spanning tree topology change occurs when you change a piggyback port.<br>• Piggyback ports display in certain views of the P550R Switch user interface where you typically expect to find information about a source port.<br>• 80 series modules do not support piggyback ports.<br>• Fabric mode 1 port mirroring works with 50 series modules. Fabric mode 2 port mirroring works with 80 series modules.<br>For example, the VLAN Switch Ports list, which displays the list of ports associated with a VLAN, includes the piggyback port but not the source port.<br>In the Intelligent Multicast Session Search and Static Multicast Sessions views, the piggyback port displays in place of the source port when piggyback port mirroring is enabled.<br>**Note:** To mirror outbound traffic only, select a source, mirror, and piggyback port. Set the sampling to disable. Since disabling sampling only applies to inbound traffic, only outbound traffic is received. |
| | ***2 of 3*** |

*Table 6-122. Port Mirroring Configuration Web Page Parameters*

| Parameter | Definition |
|---|---|
| **Sampler Type*** | Selects how often you want the mirror port to receive traffic samples:<br>• **Always** - sends all samples.<br>• **Periodic** - sends samples at the interval described below.<br>• **Disabled** - shuts off traffic samples to the mirror port, but keeps the association intact. |
| **Max Packets per Second** | Displays the number of packets per second that are served by the mirror port. |

* Sampling only applies to inbound traffic.

*3 of 3*

### Using the CLI

To set up an RMON mirror port by using the CLI, enter the following command from **Enable/Configure** mode:

```
<configure># set port mirror <mod-port-range>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1* for details about this command.

## Setting Up Port Mirroring on a Switch in Fabric Mode 2

Fabric mode 2 port mirroring provides the ability for 80-series modules to monitor traffic that a port transmits and receives. Four channels are provided for monitoring traffic, so you can monitor four different ports or port ranges simultaneously. You can set up Fabric mode 2 port mirrors by using either the Web Agent or the CLI. The switch must be in Fabric mode 2 to perform Fabric mode 2 port mirroring.

### Restrictions

*** Note:** When using Fabric mode 2 port mirroring, you cannot mirror transmit traffic of multiple source ports to one mirror port.

*** Note:** When you use Fabric mode 2 port mirroring, both the source port and mirror port must either:

— Be on the same VLAN and have the same VLAN binding

**or**

— Have VLAN binding set to **bind to all**

*** Note:** Avaya recommends that you do *not* set up a port mirror with a source port or mirror port that is bandwidth limited. This is because packets are dropped during the bandwidth limiting process. Since both source and mirror packets are subject to drop, and because packets are dropped at random, if packets are dropped from either the source or the mirror traffic (or both), there is no guarantee that the mirror traffic will match the source traffic.

*** Note:** Fabric mode 2 port mirroring is not supported for hunt group ports.

## Using the Web Agent

To use the Web Agent to set up port mirroring on a switch in Fabric mode 2:

1. Expand the **Modules & Ports** folder.
2. Click **Port Mirroring**.

   The **Port Mirroring Information** page opens (Figure 19-6). Table 6-124 provides an explanation of each field on the Web page.

***Figure 6-178. Port Mirroring Information Web Page***

Port Mirroring Information

| Channel | Source Port | Mirror Port | Direction/Filter | Sampler Type | Max Packets per Second |
|---|---|---|---|---|---|
| 1 | [None] | [None] | Receive / None | Disable | 0 |
| 2 | [None] | [None] | Receive / None | Disable | 0 |
| 3 | [None] | [None] | Receive / None | Disable | 0 |
| 4 | [None] | [None] | Receive / None | Disable | 0 |

| Channel Filter | Source MAC (SA) | Destination MAC (DA) |
|---|---|---|
| 1 | 00 :00 :00 :00 :00 :00 | 00 :00 :00 :00 :00 :00 |
| 2 | 00 :00 :00 :00 :00 :00 | 00 :00 :00 :00 :00 :00 |
| 3 | 00 :00 :00 :00 :00 :00 | 00 :00 :00 :00 :00 :00 |
| 4 | 00 :00 :00 :00 :00 :00 | 00 :00 :00 :00 :00 :00 |

APPLY

See Table 6-123, for the specific port ranges that you can mirror on each type of module.

***Table 6-123. Port Ranges for Fabric Mode 2 Port Mirroring***

| Module | Port ranges that you can mirror |
|---|---|
| 4-port gigabit modules | • 1–2<br>• 3–4<br>• Any single port<br>You can mirror any four single ports simultaneously (one port per channel). However you cannot mirror a port range and a single port within that range simultaneously.<br>**Example:** You *can* mirror port 1 on channel 1, port 2 on channel 2, and port 3 on channel 3 simultaneously. However, you *cannot* mirror ports 1 through 2 on channel 1 and port 2 on channel 2 simultaneously. |
| 8-port gigabit modules | • 1–4<br>• 5–8<br>• Any single port<br>You can mirror any four single ports simultaneously (one port per channel). However you cannot mirror a port range and a single port within that range simultaneously.<br>**Example:** You *can* mirror port 1 on channel 1, port 2 on channel 2, and port 3 on channel 3 simultaneously. However, you *cannot* mirror ports 1 through 4 on channel 1 and port 2 on channel 2 simultaneously. |
| 24-port 10/100 modules | • 1–12 — any 1 port or the entire range.<br>• 13–24 — any 1 port or the entire range.<br>If you mirror a single port, you can mirror only 1 port per range at a time.<br>**Example:** You *can* mirror port 1 on channel 1 and port 13 on channel 2 simultaneously. However, you *cannot* mirror port 1 on channel 1 and port 2 on channel 2 simultaneously. |
| | ***1 of 2*** |

*Table 6-123. Port Ranges for Fabric Mode 2 Port Mirroring*

| Module | Port ranges that you can mirror |
|---|---|
| 48-port 10/100 modules | • 1–12 — any 1 port or the entire range.<br>• 13–24 — any 1 port or the entire range.<br>• 25–36 — any 1 port or the entire range.<br>• 37–48 — any 1 port or the entire range.<br>If you mirror a single port, you can mirror only 1 port per range at a time.<br>**Example:** You *can* mirror port 1 on channel 1 and port 13 on channel 2 simultaneously. However, you *cannot* mirror port 1 on channel 1 and port 2 on channel 2 simultaneously. |
| | ***2 of 2*** |

3. Select the Channel and the associated port from the **Source Port** column pull-down menu.

4. In the **Mirror Port** column pull-down menu, select the port to which you want to mirror traffic.

   Both the source port and mirror port must either:

   — Be on the same VLAN and have the same VLAN binding

   **or**

   — Have VLAN binding set to **bind to all**

   The source port and the mirror port must be different physical ports.

5. In the **Direction/Filter** column, select the direction of traffic that you want to mirror and the filter that you want to set up, if any.

   You can set up a MAC address filter to monitor only traffic with a specific source MAC address or destination MAC address.

*** Note:** Do not set the source MAC address in the **Destination/ Filter** field.Setting a Source MAC address in the Destination MAC filter causes traffic to be improperly monitored.

6. In the **Sampler Type** column, select how often you want the mirror port to receive traffic samples.

7. Do one of the following:

| IF you select... | THEN... |
|---|---|
| **Periodic** in the **Sampler Type** column | In the **Max Packets per Second** column, enter the maximum number of packets per second that you want the mirror port to receive. |
| **Disable** or **Always** in the **Sampler Type** column | Go to step 8. |

8. If you selected **Both/DA Filter** in the **Direction/Filter** field, enter the MAC address that you want to monitor in the **DA Filter** field for the port mirror.

9. If you selected **Both/SA Filter** in the **Direction/Filter** field, enter the MAC address that you want to monitor in the **SA Filter** field for the port mirror.

10. Click **Apply**.

***Table 6-124. Port Mirroring Information Web Page Parameters***

| Parameter | Definition |
|---|---|
| **Channel** | Displays the channel number. Four channels are provided for monitoring traffic, so you can monitor four different ports or port ranges simultaneously. |
| **Source Port** | The port that you want to mirror. |
| **Mirror Port** | The port to which you want to mirror traffic.<br>Both the source port and mirror port must either:<br>• Be on the same VLAN and have the same VLAN binding<br>**or**<br>• Have VLAN binding set to **bind to all** |
| | ***1 of 2*** |

*Table 6-124. Port Mirroring Information Web Page Parameters*

| Parameter | Definition |
|---|---|
| **Direction/Filter** | The direction of traffic that you want to mirror and the filter that you want to set up, if any. Options are:<br>• **Receive/None**-Mirrors all receive traffic.<br>• **Transmit/None**-Mirrors all transmit traffic.<br>• **Both/None**-Mirrors all transmit and receive traffic.<br>• **Both/SA Filter**-Mirrors transmit and receive traffic that has the source MAC address that you specify in the **Source MAC (SA)** field.<br>• **Both/DA Filter**-Mirrors transmit and receive traffic that has the destination MAC address that you specify in the **Destination MAC (DA)** field. |
| **Sampler Type** | Specifies how often you want the mirror port to receive traffic samples. Options are:<br>• Disable<br>• Always<br>• Periodic |
| **Max Packets per Second** | The maximum number of packets per second that you want the mirror port to receive.<br>Enter a number in this field *only* if you selected **Periodic** in the **Sampler Type** field. |
| **Channel Filter** | Displays the channel number. |
| **Source MAC (SA)** | The source MAC address that you want to mirror traffic for.<br>Enter a MAC address in this field *only* if you selected **Both/SA Filter** in the **Direction/ Filter** field. |
| **Destination MAC (DA)** | The destination MAC address that you want to mirror traffic for.<br>Enter a MAC address in this field *only* if you selected **Both/DA Filter** in the **Direction/ Filter** field. |
| | ***2 of 2*** |

### CLI Command

Use the following CLI commands to configure Fabric mode 2 port mirroring. You must be in Global Configuration command mode to enter these commands.

*** Note:** For information on how to enter Global Configuration command mode, see "Accessing/Exiting the Command Modes" in Chapter 1 of *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1*.

To set up port mirroring, use the following CLI command:

<configure># set port mirror Fabric_mode2 source-port <*mod-port-range*> mirror-port <*mod-port-spec*> channel <*channel*> direction {tx | rx | both | sa | da} sampling {always | disable | periodic} [sa <*MAC-address*>] [da <*MAC-address*>] [max-packets-sec <*max-packets-sec-value*>]

For more information about this command see "set port mirror Fabric_mode2" in Chapter 19, "Port," of the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1*.

## Removing a Fabric Mode 2 Port Mirror

### Web Agent Procedure

To remove a port mirror on a switch in Fabric mode 2 by using the Web Agent:

1. Expand the **Modules & Ports** folder.
2. Click **Port Mirroring**.

   The **Port Mirroring Information** page opens.
3. In the **Source Port** column, select **None** for the port mirror that you want to remove.
4. Click **Apply**.

### Using the CLI

To remove a port mirror from a switch in Fabric mode 2, use the following CLI command from **configure** mode:

```
<configure># clear port mirror Fabric_mode2
channel <channel>
```

For more information about this command see "set port mirror Fabric_mode2" in Chapter 19, "Port," of the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, v5.3.1*.

## Viewing Information about a Fabric Mode 2 Port Mirror

### Web Agent Procedure

To view information about a Fabric mode 2 port mirror:

1. Expand the **Modules & Ports** folder.
2. Click **Port Mirroring**.

   The Port Mirroring Information page opens. This page displays information about all port mirrors that are setup.

### CLI Command

To view information about a Fabric mode 2 port mirror, use the following CLI command:

```
<configure># show port mirror Fabric_mode2
```

This command displays the source ports, mirror port, direction being mirrored, sampler type, and maximum packet per second for all port mirrors that are currently set up.

# Setting Up a Port Mirror by Using SNMP

The MIB objects that you use to configure 80-series port mirroring are located in the RFC2613 MIB and the cjnPortCopyExtensions MIB.

## Setting Up Port Mirroring

*** Note: (RN000075)** If you attempt to set up port mirroring on a port that is administratively disabled, and you configure the disabled port as a source or mirror port, note the following:

Traffic sent to a disabled source port will be lost. A disabled port set up as a mirror port will not be able to send any traffic to a monitoring device.

We recommend that you check any ports to be used in port mirroring to ensure that the ports are active.

To use SNMP to set up port mirroring:

1. Use the MIB objects that are listed in Table 6-125 to specify the port or range of ports that you want to mirror (source ports) and the port to which you want to mirror traffic (destination port).

   See Table 6-123 on page 15 for the specific port ranges that you can mirror.

***Table 6-125. MIB, MIB Objects, and OIDs for Setting Port Mirroring Sources and Destination***

| MIB | MIB Object | OID |
|---|---|---|
| RFC2613 | portCopySource | 1.3.6.1.2.1.16.22.1.3.1.1.1 |
| | portCopyDest | 1.3.6.1.2.1.16.22.1.3.1.1.2 |

Both the source port and mirror port must either:

— Be on the same VLAN and have the same VLAN binding

**or**

— Have VLAN binding set to **bind to all**

*** Note:** Avaya recommends that you mirror traffic to a port of the same speed or faster than the source port.

2. Use the MIB object that is listed in Table 6-126 to specify the direction of traffic that you want to mirror.

*Table 6-126. MIB, MIB Object, and OID for Setting the Traffic Direction to Mirror*

| MIB | MIB Object | OID |
|---|---|---|
| RFC2613 | portCopyDirection | 1.3.6.1.2.1.16.22.1.3.1.1.4 |

3. Use the MIB object that is listed in Table 6-127 to specify how often you want the mirror port to receive traffic samples.

*Table 6-127. MIB, MIB Object, and OID for Setting Port Mirroring Sampling*

| MIB | MIB Object | OID |
|---|---|---|
| cjnPortCopyExtensions | cjnPortCopySamplingMode | 1.3.6.1.4.1.6889.2.1.5.1.1.1 |

4. Use the MIB object that is listed in Table 6-128 to specify the maximum number of packets per second that you want the mirror port to receive.

*Table 6-128. MIB, MIB Object, and OID for Setting Maximum Packets Per Second*

| MIB | MIB Object | OID |
|---|---|---|
| cjnPortCopyExtensions | cjnPortCopyMaxPacketsPerSecond | 1.3.6.1.4.1.6889.2.1.5.1.1.2 |

## Removing Port Mirroring

To use SNMP to remove port mirroring, use the MIB object that is listed in Table 6-129.

*Table 6-129. MIB, MIB Objects, and OID for Removing 80-Series Port Mirroring*

| MIB | MIB Object | OID |
|---|---|---|
| RFC2613 | portCopyStatus | 1.3.6.1.2.1.16.22.1.3.1.1.5 |

### Viewing Information about Port Mirroring

To view information about port mirroring, use the MIB table that is listed in Table 6-130.

*Table 6-130. MIB, MIB Table, and OID for 80-Series Port Mirroring Information*

| MIB | MIB Table | OID |
|---|---|---|
| RFC2613 | portCopyTable | 1.3.6.1.2.1.16.22.1.3.1. |

# Enabling MAC Address Lock and Traps for Unknown Source Addresses

To enable traps for unknown source addresses, you must first enable the MAC Address Lock feature. You can enable this feature and traps for unknown source addresses by using the Web Agent, CLI, or SNMP.

### Web Agent Procedure

To use the Web Agent to enable the MAC Address Lock feature and traps for unknown source addresses:

1. Manually add the "permitted" MAC addresses to the Address Forwarding Table (AFT).

   For information on how to manually add MAC address to the AFT, see "Adding Entries to the AFT Manually" in Chapter 6, "Managing the Address Forwarding Table."

2. Open the Switch Port Configuration Web page for the port.

   For information on how to open this Web page, see "Configuring Switch Port Parameters," in Chapter 5, "Configuring Port Parameters."

3. Set the **Allow Learning** field to **Disable**.

4. Set the **Known Mode** field to **Enable**.

   *** Note:** To prevent the flooding of frames that have unknown destination addresses, set the **Known Mode** field to **Enable** for all ports on the same VLAN as the port for which you are enabling MAC address lock.

5. Set the **Intrusion Trap** field to **Enable**.

6. Adjust the trap timer, if desired.

   See "Configuring Switch Port Parameters" in Chapter 5, "Configuring Port Parameters," for information on how to perform these procedures.

7. Click **Apply**.

## CLI Commands

To use the CLI to enable the MAC Address Lock feature and traps for unknown source addresses:

1. Enter **Global Configuration** mode.

   The CLI displays the **<configure>#** prompt.

2. Use the following command to manually add the "permitted" MAC addresses to the Address Forwarding Table (AFT):

   **set aft entry <*mac address*> vlan <*vlan-id*> port-binding forward <*mod-port-spec*>**

3. Use the following command to disable learning on a port or port range:

   **set port allow-learning <*mod-swport-range*> disable**

4. Use the following command to enable known mode on a port or port range:

   **set port known-mode <*mod-swport-range*> enable**

   *** Note:** To prevent the flooding of frames that have unknown destination addresses, enter all ports on the same VLAN as the port for which you are enabling MAC address lock.

5. Use the following command to enable intrusion traps on a port or port range:

   **set port intrusion-trap <*mod-swport-range*> enable**

6. Use the following command to set the intrusion trap timer to other than the default setting:

   **set port intrusion-trap-timer <*mod-swport-range*> <*intrusion-trap-timer-value*>**

## SNMP MIB Objects

The MIB objects that you use to perform this procedure are located in **ProminetMib.txt**, version 5.2.

To use SNMP to enable the MAC Address Lock feature and traps for unknown source addresses:

1. Use the MIB objects that are listed in Table 6-131 to manually add the "permitted" MAC addresses to the AFT.

*Table 6-131. MIB, MIB Objects, and OIDs for Adding AFT Entries*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.3 | promL2AddressControlIndex | 1.3.6.1.4.1.2167.5.1.4.3.1.1 |
| | promL2AddressControlMacAddress | 1.3.6.1.4.1.2167.5.1.4.3.1.2 |
| | promL2AddressControlPortBinding | 1.3.6.1.4.1.2167.5.1.4.3.1.3 |
| | promL2AddressControlVlanID | 1.3.6.1.4.1.2167.5.1.4.3.1.4 |
| | promL2AddressControlPriority | 1.3.6.1.4.1.2167.5.1.4.3.1.5 |
| | promL2AddressControlPersistence | 1.3.6.1.4.1.2167.5.1.4.3.1.6 |

2. Use the MIB object that is listed in Table 6-132 to disable learning on a port.

*Table 6-132. MIB, MIB Object, and OID for Disabling Learning*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.3 | promSwitchPortLearningMode | 1.3.6.1.4.1.2167.5.2.1.1.4 |

3. Use the MIB object that is listed in Table 6-133 to enable known mode on a port.

*Table 6-133. MIB, MIB Object, and OID for Enabling Known Mode*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.3 | promSwitchPortKnownMode | 1.3.6.1.4.1.2167.5.2.1.1.7 |

4. Use the MIB object that is listed in Table 6-134 to enable intrusion traps on a port

.

*Table 6-134. MIB, MIB Object, and OID for Enabling Intrusion Traps*

| MIB | MIB Object | OID |
|---|---|---|
| **ProminetMib.txt**, version 5.3 | promSwitchPortIntrusionTrap | 1.3.6.1.4.1.2167.5.2.1.1.19 |

# 20 Managing Buffers and Queues on 50-Series Modules

## Overview

The following information and procedures provided in this chapter pertain to layer 2 and layer 3 module configurations. Buffer management features help you to optimize traffic throughput through the switch fabric.

This chapter provides the following information:

- How Queues Work
- Managing Buffers and Queues

## How Queues Work

Frames are buffered in the I/O modules, before and after traversing the switch. Each queue can hold 256K bytes. (Architecturally they can support up to 1 MB each).

Each buffer is divided into two queues, one for High-priority Traffic and one for Normal-priority Traffic. The factory default is for the high-priority queue uses 20% (51K) of the buffer. The normal-priority queue uses the remaining 80% (205K). These values can be modified using either the Web Agent or SNMP.

*** Note:** When you change these values, you must reboot the switch before they can take effect.

Less buffer memory gets assigned to the high-priority queue because the high-priority queue gets serviced more frequently than the normal-priority queue. Since a frame spends less time on the high-priority queue, less buffer space is required for the queue.

The Service Ratio can be chosen to match traffic patterns and performance requirements using a weighted round robin scheduling algorithm. The available service ratios of the algorithm are defined in "*Managing Buffers and Queues*". The factory default service ratio for fabric ports is 999/1. The factory default service ratio for physical

ports is 1023 to 1. If there is traffic to be serviced from both the high- and normal-priority queues, 999 packets of high-priority traffic will be processed for each normal-priority packet.

When the high-priority queue fills up, incoming frames are dropped. The philosophy is if a high-priority frame is going to be late, it is not worth sending it at all. The normal-priority queue uses either IEEE 802.3X PAUSE (variable timed XOFF) flow control or Half Duplex collisions to shut off incoming frames before the queue overflows.

The switch implements two flow control disciplines along the entire path that frames travel. The default case is that when output buffers fill up, frames destined for a particular buffer will be dropped. This should only occur in a case where the output port is very congested. However, there is an optional mode in which normal-priority frames are never dropped inside the switch. In this mode, input buffers may fill up. If they do, the affected input ports may use flow control to temporarily halt traffic from neighboring switches.

# Managing Buffers and Queues

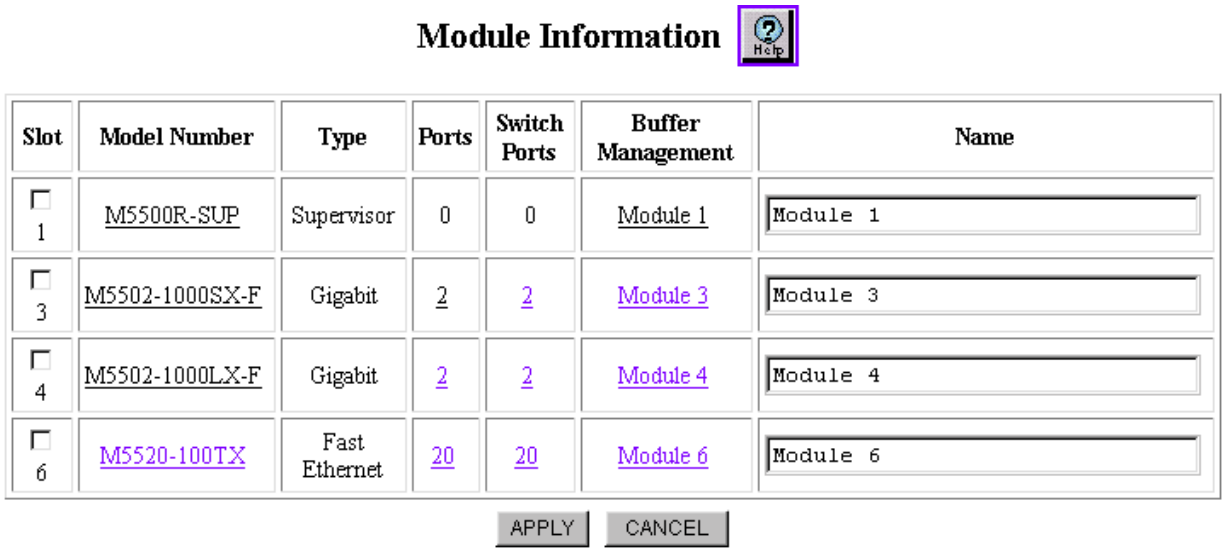
You can manage buffers and queues using either the Web Agent or the CLI.

## Managing Buffers and Queues Using the Web Agent

To manage buffers and queues using the Web Agent:

1. Select **Configuration** from the **Modules & Ports** group on the Web Agent window. The **Module Information** dialog box opens (Figure 6-179).

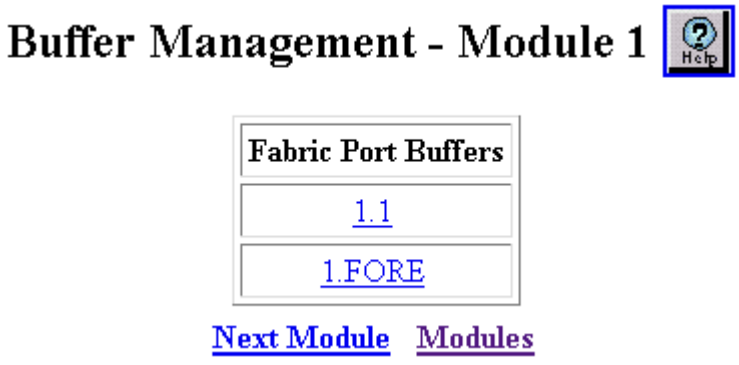
*Figure 6-179. Module Information Dialog Box*




2. Select the module whose buffers you want to manage from the **Select** column.

3. Select the Module number for that module from the Buffer Management column. The **Buffer Management** dialog box opens (Figure 6-180).

*Figure 6-180. Buffer Management Dialog Box*



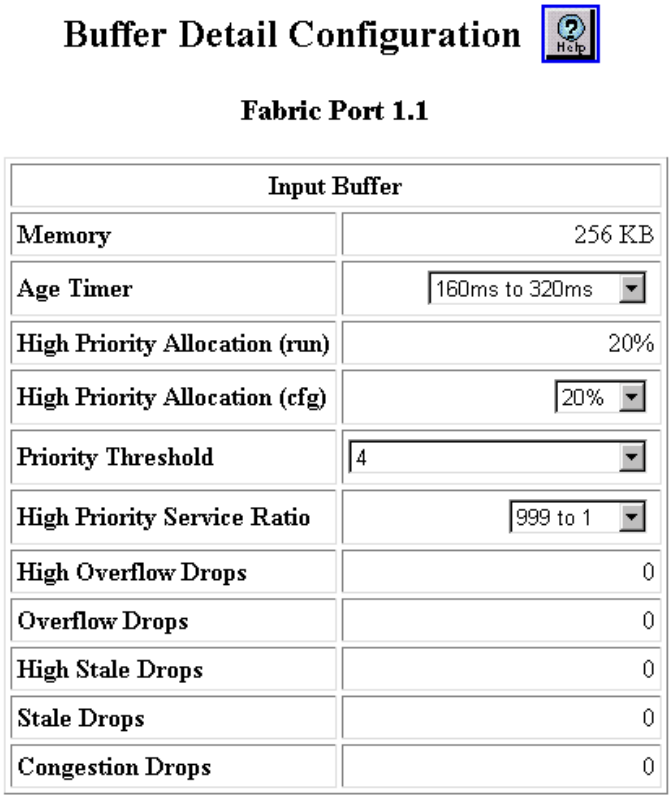
4. Refer to Table 4 for an explanation of the Buffer Management dialog box parameters.

*Table 6-135. Buffer Management Dialog Box Parameters*

| Parameter | Definition |
|---|---|
| **Fabric Port Buffers** | Displays the port's fabric port buffers and allows you to open the **Buffer Detail Configuration** dialog box for the selected module.<br>Service ratios:<br>• 3 to 1<br>• 99 to 1<br>• 999 to 1<br>• 9999 to 1 |
| **Physical Port Buffers** | Displays the port's physical port buffers if available. The buffer ratios are:<br>• 31 to 1<br>• 63 to 1<br>• 127 to 1<br>• 255 to 1<br>• 511 to 1<br>• 1023 to 1<br>• 2047 to 1<br>• 4095 to 1<br>• 8191 to 1<br>• 16383 to 1<br>• 32767 to 1 |

5. Select the Fabric Port Buffer number whose associated buffers you want to manage. The **Buffer Detail Configuration** dialog box for that fabric port opens (Figure 6-181).

*Figure 6-181. Buffer Detail Configuration Dialog Box*




6. Refer to Table 6-136 for an explanation of the **Buffer Detail Configuration** dialog box input and output fields:

*Table 6-136. Buffer Detail Configuration Dialog Box Parameters*

| Parameter | Definition ... |
|---|---|
| **Memory** | Displays the amount of physical memory associated with this buffer. |
| **Age Timer** | Displays the amount of time a packet remains in the queue before being discarded as a stale packet. You may want to increase the timer value for ports connected to 10 MB/s ports, particularly 10 MB/s shared media, because you may want to queue packets longer before discarding them. |

*Table 6-136. Buffer Detail Configuration Dialog Box*

| Parameter | Definition ... |
|---|---|
| **High Priority Allocation** | Displays the percent of the buffer's queuing space allotted to high priority traffic. Because the high-priority queue is serviced more frequently than the normal priority queue, raising this value may not necessarily provide better service. In fact, if you are using the high-priority queue for delay-sensitive traffic, you may want to reduce the amount of memory devoted to the high-priority queue. This ensures that packets that cannot be delivered in a timely manner are discarded. If you want the high priority queue to guarantee delivery of as many packets as possible, regardless of delay, increase this value. The change does not take effect until you reset the switch. |
| **Priority Threshold** | Allows you to set this parameter to the value at which the P550R switch starts sending packets to the high-priority queue. The default value (4) causes all traffic with a priority greater than or equal to 4 (4, 5, 6, and 7) to be assigned to the high-priority queue. Priority schemes have more than two queues (the IEEE allows up to 8, numbered 0 through 7). Avaya recommends that you do not change this parameter. |
| **High Priority Service Ratio** | Allows you to set how many times the high priority queue is serviced for each time the low priority queue is serviced. The ideal value changes from queue to queue, but the goal is to ensure that traffic mix guarantees optimal mix between high-priority and best effort traffic. |
| **High and Normal Overflow Drops** | Displays the number of packets dropped because the associated buffer is full. Indicates that the device immediately before the queue is processing traffic faster than the next downstream element can process the same volume of traffic. For example, overflow drops on the input buffer indicate that traffic is arriving faster than the switch matrix can process it. Overflow drops on the output buffers indicates that the output port cannot handle the volume of the load being offered. |
| **High and Normal Stale Drops** | Displays the number of packets dropped because they timed out waiting for service (using the age timer value). In the high-priority queue, this can help determine how efficiently the switch is processing "better never than late" traffic. Excessive stale drops on the high-priority queue may indicate the need to increase the service ratio on the high-priority queue. |
| **Congestion Drops** | Displays the number of packets dropped because the switch controller has sensed congestion at the outbound port. |

7. Repeat Steps 1-4 to tune Physical Port (Fast Ethernet) buffers. Physical Port ports have additional buffers on both the input and output ports.

8. Click **APPLY** to save your changes, or **CANCEL** to restore previous settings.

## Managing Buffers and Queues Using the CLI

To manage buffers and queues using the CLI, enter the following command from **Configure** mode:

```
(configure)# set buffering port <mod-swport-spec>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

# 21 80-Series QoS

## Overview

Quality of Service (QoS) is a set of tools that make it possible for you to manage traffic across a switch or a network. These tools protect specific traffic from the effects of network congestion. You can enable these features for a module or individual ports on a module to control the flow of traffic across your network. This control makes it possible for you to guarantee that delay-sensitive traffic such as voice over IP (VoIP) receives the priority it requires, while also ensuring that the switch services other low priority data.

The QoS features are supported only on 80-series modules. Fifty-series modules do not support these features.

This chapter contains the following sections:


- "Why implement QoS?" on page 2
- "How Does QoS Work?" on page 3
- "Classification of Traffic" on page 7
- "Ingress Policing" on page 31
- "Queue-Servicing Algorithms" on page 35
- "QoS Statistics" on page 47


*** Note:** In this release, you can configure the QoS features only by using the CLI or Avaya Policy Manager Version 2.2. These features are not available in the Web Agent or SNMP.

# Why implement QoS?

## Purpose of QoS

In a network that has time-sensitive traffic (VoIP) or bandwidth-intensive traffic (real-time or near-real-time streaming-video), QoS makes it possible for you to prioritize the time-sensitive traffic and assign larger amounts of bandwidth to those applications that require it.

VoIP traffic has relatively low bandwidth requirements, but cannot tolerate latency or frame loss. Therefore, this traffic needs a high priority to ensure its timely delivery. On the other hand, streaming video is bandwidth-intensive but has large “jitter buffers” so can tolerate some latency. Thus, you can assign streaming video traffic a lower priority than voice, but must assign streaming video more bandwidth than voice.

## Prerequisites

To successfully implement QoS, you must have a thorough knowledge of the traffic patterns in the network. You need this information to:

- Classify traffic and assign it the required priority and bandwidth.
- Identify the areas of the network where bottlenecks might occur and that therefore need bandwidth limiting.
- Identify the areas of the network where time-sensitive traffic is being delayed and needs to be prioritized better.

## Implementation Example

An example of managing QoS across the network is to define traffic classes and manage these on a network-wide basis. The four classes and their priorities might look like those outlined in Table 6-137

*** Note:** For information about DSCP (DiffServ Code Point), see “Diffserv” on page 10.

***Table 6-137. Examples of Classes of Service***

| Service Class | Priority | DSCP Value | Type of Traffic |
|---|---|---|---|
| Highest Priority | 7 | 56 | Network Management Traffic, OSPF, Spanning Tree, etc. |
| Time Sensitive Traffic | 5 | 40 | Real-time voice, video conferences. |

***1 of 2***

*Table 6-137. Examples of Classes of Service*

| Service Class | Priority | DSCP Value | Type of Traffic |
|---|---|---|---|
| High Priority Data | 1 | 8 | SAP, Web, etc. Dependent upon your business. |
| Best Effort | 0 | 0 | Everything else. |
| | | | *2 of 2* |

# How Does QoS Work?

The QoS process starts at the point where a frame enters the switch and ends when the frame exits the switch. This section describes the QoS process from start to finish.

## QoS Process for Ingress Traffic

### Process

The QoS process for ingress traffic involves the following steps:

1. Identifying the priority, also called *class*, of the frame or packet. The switch can identify the priority of the frame or packet by using one or more of the following criteria:
   - The priority of the physical port that the switch received the frame or packet on
   - Cisco ISL tag priority
   - 802.1p tag priority (default)
   - The source or destination MAC address
   - The DiffServ code point
   - The IP protocol (assigned by means of an ACL rule)
   - The source or destination IP address (assigned by means of an ACL rule)
   - The source or destination TCP or UDP port (assigned by means of an ACL rule)

   For more information on identifying the priority of traffic, see “Classification of Traffic” on page 7.

2. Storing the frame or packet in one of eight ingress queues.

   The switch stores the frame or packet in the queue that matches the priority that was identified in Step 1.

3. Forwarding the frame or packet from the ingress queue to its destination.

   If you enable *policing* for the queue, the switch forwards ingress traffic that falls within the maximum bit rate that you set and drops ingress traffic that exceeds the maximum bit rate. For more information on policing, see "Ingress Policing" on page 31.

### Example

You want to assign a priority of 5 to a VoIP flow that is destined to an IP 600 phone switch. You also want to police the port that receives the VoIP data to 5 Mbps.

1. You set up an ACL rule that associates a priority of 5 with the destination IP address of the VoIP flow. (VoIP traffic cannot tolerate latency or frame loss, so it needs a high priority to ensure its timely delivery.)

   ***Note:** Priority 5 serves as an example only. Actual implementations may vary.

2. You enable policing on the port that will receive the VoIP flow and set the guaranteed bit rate to 5 Mbps.

3. The switch stores packets that match the ACL rule in queue 5. (The switch stores packets in the queue that matches their priority.)

4. The switch forwards the VoIP traffic in queue 5 as long as its bit rate does not exceed 5 Mbps. If the bit rate of the queue exceeds 5 Mbps, the switch drops the excess traffic.

## QoS Process for Egress Traffic

### Process

The QoS process for egress traffic involves the following steps:

1. Storing the frame or packet in one of eight egress queues.

   The switch stores the frame or packet in the queue that matches the priority that was identified on the ingress port.

2. Forwarding the frame or packet from the queue to the egress port for transmission.

   The switch uses algorithms that allocate bandwidth among the egress queues to forward the traffic in the queues. The Avaya Multiservice switch software supports the following queue-servicing algorithms for egress ports:

   — Weighted fair queuing (WFQ)

   — Class-based queuing (CBQ)

   — Class-based weighted fair queuing (CBWFQ)

   — Strict Priority Queuing

## Example

You want to assign a priority of 5 to a VoIP flow that is destined to an IP 600 phone switch. You then want the switch to use the CBWFQ queue-servicing algorithm to forward frames from queue 5. The IP 600 phone switch is connected to an Avaya P882 Multiservice switch on port 5.5.

1. You set up an ACL rule that associates a priority of 5 with the destination IP address of the VoIP flow. (VoIP traffic cannot tolerate latency or frame loss, so it needs a high priority to ensure its timely delivery.)

   ***Note:** Priority 5 serves as an example only. Actual implementations may vary.

2. You enable CBWFQ for queue 5 on port 5.5.

3. The switch assigns a priority of 5 to the ingress VoIP packets and forwards them through ingress queue 5 to the egress port.

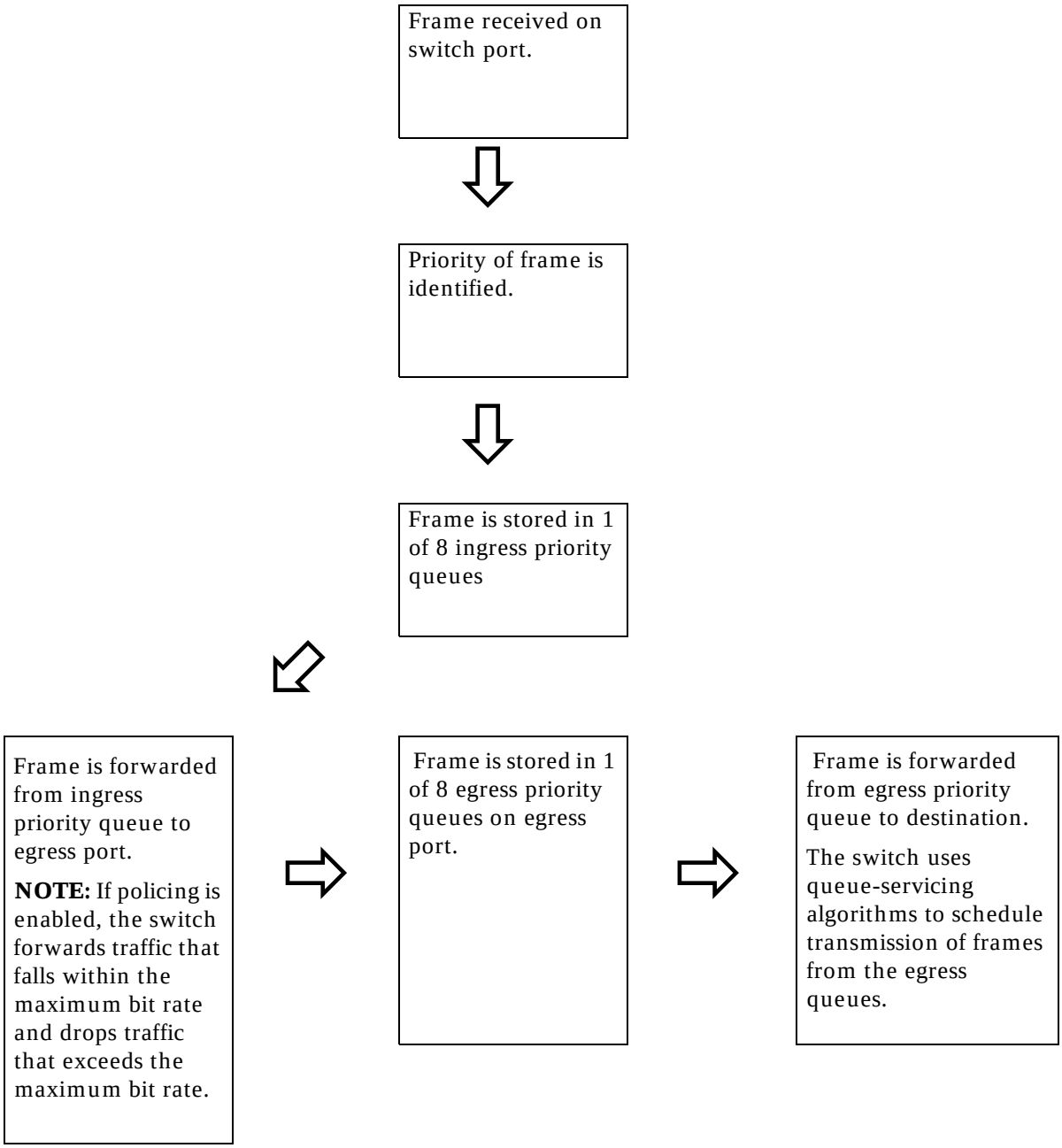
4. The switch stores the VoIP packets in egress queue 5 on port 5.5. (The switch places packets in the queue that matches their priority.)

5. The switch uses the CBWFQ algorithm to remove the packets from queue 5 and forward them to the IP 600 phone switch.

# Diagram of QoS Process

Figure 6-182 illustrates the QoS process from when a frame enters the switch to when the frame exits the switch.

***Figure 6-182. QoS Process***


Frame received on switch port.
Priority of frame is identified.
Frame is stored in 1 of 8 ingress priority queues
Frame is forwarded from ingress priority queue to egress port.
NOTE: If policing is enabled, the switch forwards traffic that falls within the maximum bit rate and drops traffic that exceeds the maximum bit rate.
Frame is stored in 1 of 8 egress priority queues on egress port.
Frame is forwarded from egress priority queue to destination.
The switch uses queue-servicing algorithms to schedule transmission of frames from the egress queues.

# Classification of Traffic

The switch assigns traffic to one of eight queues according to the priority, or "class," of the traffic. Priorities range 0 to 7, 7 being the highest priority. You can set the switch to classify traffic by the priority assigned to the following characteristics:

- Layer 2 characteristics:
  - Physical port that the frame or packet is received on
  - Cisco ISL tag or 802.1p tag
  - Source MAC address
  - Destination MAC address
- Layer 3 characteristics:
  - DSCP in the packet
  - New DSCP that replaces the original DSCP. You specify this new DSCP.
  - IP protocol (assigned by means of an ACL rule)
  - Destination IP address (assigned by means of an ACL rule)
  - Source IP address (assigned by means of an ACL rule)
- Layer 4 characteristics:
  - Destination TCP or UDP port (assigned by means of an ACL rule)
  - Source TCP or UDP port (assigned by means of an ACL rule)

## Default Priority

By default, the switch uses the priority from the 802.1p tag field, if present, to classify a frame.

If you do not change any of the QoS default settings and the frame does not have an 802.1 tag or Cisco ISL tag, the switch assigns the priority of the physical port to the packet. Each physical port has a default priority of 3. For information on how to change the priority for a physical port, see "Setting the Priority of a Physical Port" on page 13.

However, the priority of the 802.1 tag and Cisco ISL tag take precedence over the priority of the physical port, so the switch uses the priority of the physical port *only* if:

- No tags are present in the frame

  **or**

- You have set the physical port to ignore priorities in tags.

  For information on how to set a port to ignore priorities in tags, see "Setting a Physical Port to Ignore Tag Priority" on page 14.

## Classifying Traffic by Layer 2 Characteristics

In addition to Cisco ISL tag, 802.1p tag, and physical port priority, the switch can classify traffic by:

- Source MAC address
- Destination MAC address

For information about how to set a priority for a source or destination MAC address, see "Setting the Priority of a MAC Address" on page 16.

In addition to these layer 2 characteristics, you can classify bridged IP traffic by DiffServ code point. For more information on classifying bridged IP traffic by DiffServ code point, see "Diffserv" on page 10.

## Classifying Traffic by Layer 3 or Layer 4 Characteristics

### ACL Rules

You can, alternately, configure the switch to classify traffic by the IP characteristics of packets, instead of 802.1p tag priority, physical port priority, or other layer 2 characteristics.

To assign priorities to packets by their IP characteristics, you create a rule in an access control list (ACL). The rule can:

- Set an ACL rule priority
- Use the DiffServ code point
- Mask the three least significant bits of the DSCP. The switch recognizes the remaining bits as the IP precedence field.

- Replace the existing DSCP with a DSCP that you specify
- Use the layer 2 priority

You can specify the TCP/IP traffic that you want the rule to apply to. The rule can apply to traffic with a specific:

- IP destination address
- IP source address
- IP Protocol
- Destination TCP or UDP port
- Source TCP or UDP port

The priority that is specified by an ACL takes precedence over all other priorities. Because of this precedence, the switch determines whether a rule in an ACL exists for an IP packet in the final stage of classification. If an ACL exists, the priority associated with the ACL replaces the current priority of the frame.

For information on how to set a rule in an ACL, see "Setting Up an ACL Rule" on page 23.

## Using a Default ACL Rule

By default, the switch classifies packets by their layer 2 priority, if they do not match an ACL rule. However, you can set up a *default ACL rule* that the switch will apply to all packets that do match any other ACL rules. This default ACL rule sets a default characteristic, other than the layer 2 priority, that the switch will use to classify the packets.

For example, if you set up the following ACL rules:

- access-list List1 1 fwd2 10.10.60.0 0.0.0.255
- access-list List1 2 fwd4 10.10.70.0 0.0.0.255
- access-list List1 3 permit use-priority 4 10.10.80.0 0.0.0.255
- access-list List1 4 permit use-priority 6 10.10.90.0 0.0.0.255
- access-list List1 5 fwd1 10.10.100.0 0.0.0.255
- access-list List1 6 fwd4 10.10.110.0 0.0.0.255
- access-list List1 7 fwd7 10.10.120.0 0.0.0.255
- access-list List1 8 fwd8 10.10.130.0 0.0.0.255
- access-list List1 512 permit use-priority 6 any (default ACL rule)

All packets that have a source IP address in the 10.10.60 subnet are assigned a priority of 1(fwd*x* is 1 based, but priorities are 0 based.) All packets that have a source IP address in the 10.10.70 subnet are assigned a priority of 3, and so on. Any packets whose source IP addresses do not match the IP addresses in ACL rules one through eight, are assigned a priority of 6.

For information on how to set up a default ACL rule, see "Setting Up a Default ACL Rule" on page 30.

## Diffserv

RFC 2475 defines a field in the layer 3 header of IP packets, called the DiffServ code point (DSCP). Typically, hosts or routers sending traffic into a DiffServ network mark each transmitted packet with the appropriate DSCP. The switch then uses the DSCP to classify packets. You can alternately set the switch to replace the DSCP in a packet with a different DSCP. The switch then uses the new DSCP to classify the packet.

To set the switch to classify IP packets by their DSCP or to replace the DSCP with a different DSCP, you must set up an ACL rule. For information on how to set up an ACL rule to enable DiffServ functionality, see "Setting Up an ACL Rule" on page 23.

The Differentiated Services (DiffServ) Mapping Table associates specific DSCP values with specific priorities. You create these associations by assigning priorities to DSCPs. For information on how to assign priorities to DSCPs, see "Assigning a Priority to a DSCP" on page 21.

Because the DSCP is located in the layer 3 header, the switch does not typically use the DSCP to classify bridged IP traffic. However, you can set a physical port to use the DSCP to classify bridged IP traffic. For information on how to set a physical port to use DiffServ, see "Setting a Physical Port to Use DiffServ" on page 19.

# Precedence of Priorities

If multiple priorities are associated with a frame or packet, the switch classifies the frame or packet according to the priority of highest precedence. See Table 6-138 for the precedence of each priority.

The switch then assigns the frame or packet to the appropriate priority queue based on the priority of the frames.

***Table 6-138. Precedence of Priorities***

| Layer | Precedence of Priority | Priority Used for Classification |
|---|---|---|
| **Layer 3** | | |
| | High | ACL rule priority |
| | | DSCP in the packet or DSCP that the switch replaces the original DSCP with |
| **Layer 2** | | |
| | | DSCP (for bridged IP traffic) |
| | | Destination MAC address priority |
| | | Source MAC address priority |
| | | 802.1p tag |
| | | Cisco ISL tag |
| | Low | Physical port priority |
| | | |

# Supported Number of Queues

Table 6-139 specifies the number of ingress and egress queues that are available on each module.

***Table 6-139. Modules and Available Queues***

| Module | Ingress Queues | Egress Queues |
|---|---|---|
| 4-port gigabit modules | 1 set of 8 queues per port<br>**Total:** 4 sets of 8 queues | 1 set of 8 queues per port<br>**Total:** 4 sets of 8 queues |
| 8-port gigabit modules | 1 set of 8 queues per port<br>**Total:** 8 sets of 8 queues | 1 set of 8 queues per port<br>**Total:** 8 sets of 8 queues |
| 24-port 10/100 modules | • 1 set of 8 queues for ports 1–12.<br>• 1 set of 8 queues for ports 13–24.<br>**Total:** 2 sets of 8 queues | 1 set of 8 queues per port.<br>**Total:** 24 sets of 8 queues |
| 48-port 10/100 modules | • 1 set of 8 queues for ports 1–12.<br>• 1 set of 8 queues for ports 13–24.<br>• 1 set of 8 queues for ports 25–36<br>• 1 set of 8 queues for ports 37–48<br>**Total:** 4 sets of 8 queues | 1 set of 8 queues per port.<br>**Total:** 48 sets of 8 queues. |

# Setting the Priority of a Physical Port

## Command

Use the **set port default-priority** command to set the priority of a physical port. Each physical port has a default priority of 3. The syntax of the command is:

Avaya(configure)#set port default-priority {{<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] | all-ports} <*priority*>

***Table 6-140. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, the priority is set for all ports on the module. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the priority is set for the port or range of ports on the module that you specify. |
| all-ports | All ports in the chassis. If you specify **all-ports**, all ports on all modules in the chassis are set with the same priority. |
| <*priority*> | The priority that you want to assign to the port or port range. Enter a number between 0 and 7. The highest priority is 7. Each physical port has a default priority of 3. |
| | |

## Examples

*Table 6-141. Examples: set port default-priority*

| To . . . | Enter . . . |
|---|---|
| Set the port priority to 0 for all ports on the module in slot 3 | **set port default-priority 3 0** |
| Set the port priority to 5 for ports 1 through 5 on the module in slot 3 | **set port default-priority 3/1-5 5** |
| Set the port priority to 2 for ports 1 through 5 on the module in slot 3 and for port 1 on the module in slot 6 | **set port default-priority 3/1-5,6/1 2** |
| | |

# Setting a Physical Port to Ignore Tag Priority

## Command

Use the **set port ignore-tag priority** command to set a port to ignore any layer 2 tag priority (including 802.1p tags). The syntax of the command is:

Avaya(configure)#set port ignore-tag-priority {{<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] | all-ports} {on | off}

*Table 6-142. Keywords, Arguments, or Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, the switch ignores tag priorities on all ports of the module. |
| | ***1 of 2*** |

*Table 6-142. Keywords, Arguments, or Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the switch ignores tag priorities on the port or range of ports on the module in the slot that you specify. |
| all-ports | All ports in the chassis. If you specify **all-ports**, all ports on all modules in the chassis are set with the same priority. |
| {on \| off} | Indicates whether you want the port to ignore tag priority. Enter **on** for the port to ignore the tag priority.<br>The default setting is **off**. |
| | ***2 of 2*** |

## Examples

*Table 6-143. Examples: set port ignore-tag-priority*

| To . . . | Enter . . . |
|---|---|
| Set all ports on the module in slot 3 to ignore the 802.1p tag priority | **set port ignore-tag-priority 3 on** |
| Set ports 1 through 5 on the module in slot 3 to *not* ignore the 802.1p tag priority | **set port ignore-tag-priority 3/1-5 off** |
| Set ports 1 through 5 on the module in slot 3 and port 1 on the module in slot 6 to ignore the 802.1p tag priority | **set port ignore-tag-priority 3/1-5,6/1 on** |
| | |

# Setting the Priority of a MAC Address

## Command

Use the **set aft entry** command to set the priority of a source MAC address or destination MAC address. The syntax of the command is:

Avaya(configure)#set aft entry <*mac-address*> vlan {<*vlan-id*> | name <*vlan-name*>} port-binding {filter | forward <*mod-port-spec*>} [persistence {ageout | permanent}] [priority {normal | high}] [sa-priority {port | aft <*entry-priority*> | max-port-aft <*entry-priority*>}] [da-priority {port | aft <*entry-priority*> | max-port-aft <*entry-priority*>}]

***Table 6-144. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| sa-priority port | Uses the priority of the physical port, Cisco ISL tag, or 802.1p tag to determine the layer 2 priority of frames. |
| sa-priority aft | Uses the priority that is assigned to the source MAC address in the Address Forwarding Table (AFT) to determine the layer 2 priority of frames. |
| <*entry-priority*> | The priority that you want to assign to the source MAC address. Enter a number between 0 and 7. This priority is stored in the AFT entry for the MAC address that you specify. |
| sa-priority max-port-aft | Determines the priority of a frame by using the higher of the:<br>• Physical port priority or tag priority<br>• Source MAC address priority |
| da-priority port | Uses the priority of the physical port, Cisco ISL tag, 802.1p tag, or source MAC address to determine the layer 2 priority of frames. |
| da-priority aft | Uses the priority that is assigned to the destination MAC address in the AFT to determine the priority of the frame. |
| <*entry-priority*> | The priority that you want to assign to the destination MAC address. Enter a number between 0 and 7. |
| | ***1 of 2*** |

*Table 6-144. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| da-priority max-port-aft | Determines the priority of the frame by using the higher of the:<br>• Physical port priority or tag priority<br>• Destination MAC address priority |
| | *2 of 2* |

For definitions of all other keywords, arguments, and options in this command, see "set aft entry" in Chapter 2, "AFT," of *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

## Examples

*Table 6-145. Examples: set aft entry*

| To . . . | Enter . . . |
|---|---|
| • Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.<br>• Forward frames that have a source or destination MAC address of 00:00:00:00:00:55.<br>• Assign a priority of 7 to frames that have a source MAC address of 00:00:00:00:00:55. | **set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 sa-priority aft 7** |
| • Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.<br>• Forward frames that have a source or destination MAC address of 00:00:00:00:00:55.<br>• Associate a priority of 5 with the source MAC address of 0:00:00:00:00:55.<br>• Assign the higher of the port priority, tag priority, or source MAC address priority (5) to frames that have a source MAC address of 00:00:00:00:00:55. | **set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 sa-priority max-port-aft 5** |
| | *1 of 2* |

*Table 6-145. Examples: set aft entry*

| To . . . | Enter . . . |
|---|---|
| • Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.<br>• Forward frames that have a source or destination MAC address of 00:00:00:00:00:55.<br>• Assign a priority of 7 to packets that have a destination MAC address of 00:00:00:00:00:55. | **set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 da-priority aft 7** |
| • Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.<br>• Forward frames that have a source or destination MAC address of 00:00:00:00:00:55.<br>• Associate a priority of 5 with the destination MAC of address 0:00:00:00:00:55.<br>• Assign the higher of the port priority, tag priority, or destination MAC address priority (5) to frames that have a destination MAC address of 00:00:00:00:00:55. | **set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 da-priority max-port-aft 5** |
| | ***2 of 2*** |

# Displaying the Priority of a MAC Address

## Command

Use the **show aft entry** command to display the priority of a source MAC address or destination MAC address. The syntax of the command is:

Avaya>show aft entry [mac <*wildcard-mac-address*>] [VLAN {<*VLAN-id*> | name <*VLAN-name*>}] [port-binding {cpu | filter | forward [<*mod-port-spec*>]}] [status {learned | management | self | multicast}]

For more information about this command, see Chapter 2, “AFT,” in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

# Setting a Physical Port to Use DiffServ

## Command

Use the **set port use-diffserv** command to set a port to classify bridged IP traffic by its DiffServ code point (DSCP). The syntax for the command is:

Avaya(configure)#set port use-diffserv {{<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] | all-ports} {on | off}

***Table 6-146. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, all ports on the module are set to use DiffServ. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the port or range of ports on the module that you specify is set to use DiffServ. |
| {all-ports} | All ports in the chassis. If you enter **all-ports**, all ports in the chassis are set to use DiffServ. |
| {on \| off} | Indicates whether the switch uses the DSCP to classify bridged IP traffic on the ports that you specify:<br>• Enter **on** to classify traffic by DSCP.<br>• Enter **off** to ignore the DSCP.<br>The default setting is **off**. |
| | |

## Example

To set ports 4 through 12 on the module in slot 6 to classify bridged IP traffic by DSCP, enter:

**set port use-diffserv 6/4-12 on**

# Setting a Physical Port to Mask DiffServ Bits

## Command

Use the **set port mask-diffserv** command to mask the three least significant bits of the DSCP when the switch is using the DSCP to classify bridged IP traffic. If you mask the three least significant bits of the DSCP, the switch recognizes the remaining bits as the precedence field of the type of service (TOS) field and classifies the packets accordingly.

The syntax of this command is:

Avaya(configure)#set port mask-diffserv {{<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] | all-ports} {on | off}

***Table 6-147. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, all ports on the module mask the three least significant bits of the DSCP. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the port or range of ports on the module that you specify mask the three least significant bits of the DSCP. |
| {all-ports} | All ports in the chassis. If you enter **all-ports**, all ports in the chassis are set to mask the three least significant bits of the DSCP. |
| | ***1 of 2*** |

*Table 6-147. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| {on \| off} | Indicates whether the switch masks the three least significant bits of the DSCP:<br>• Enter **on** to mask the bits.<br>• Enter **off** to not mask the bits.<br>The default setting is **off**. |
| | *2 of 2* |

### Example

To set all ports on the module in slot 3 to mask the three least significant bits of the DSCP, enter:

**set port mask-diffserv 3 on**

## Assigning a Priority to a DSCP

### Command

Use the **set diffserv priority** command to assign a priority to a DiffServ code point (DSCP) in the DiffServ Mapping Table. The syntax of the command is:

Avaya(configure)#set diffserv priority <*priority*> dscp <*dscp-start-range*> [<*dscp-end-range*>]

*Table 6-148. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*priority*> | The priority that you want to assign. Enter a number between 0 and 7. |
| <*dscp-start-range*> | The first DSCP in the range of DSCPs that you want to assign the priority to. DSCPs range from 0 to 63. |
| [<*dscp-end-range*>] | The last DSCP in the range of DSCPs that you want to assign the priority to. DSCPs range from 0 to 63. |
| | |

### Example

To assign a priority of 7 to DSCPs 15 through 63, enter:

**set diffserv priority 7 dscp 15 63**

# Displaying the DiffServ Table

## Command

Use the **show diffserv table** command to display the priority that is assigned to each DSCP.

The syntax of the command is:

Avaya>show diffserv table

*** Note:** The **show diffserv table** CLI command displays the packet loss probability (PLP) for each DSCP. However, the switch does not currently support PLP.

# Displaying the QoS Settings for a Physical Port

## Command

Use the **show port** command to display the QoS settings for a physical port. This command displays the priority of the port, if the port is set to ignore 802.1p tag priority, and if the port is set to use the DSCP for bridged IP traffic.

The syntax of the command is:

Avaya>show port [{<*mod-num*> | <*mod-swport-range*>} [...,{<*mod-num*> | <*mod-swport-range*>}]]

***Table 6-149. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, the switch displays the QoS settings for all ports on the module in the slot that you specify. |
| | ***1 of 2*** |

*Table 6-149. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the switch displays the QoS settings for the port or range of ports on the module in the slot that you specify. |
| | ***2 of 2*** |

For more information about this command, see Chapter 19, "Port," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

# Setting Up an ACL Rule

## Command

Use the **access list** command to set a rule in an access control list. The rule that you set up will be applied on all of the ports on the switch. For more information about using ACL rules, see "Classifying Traffic by Layer 3 or Layer 4 Characteristics" on page 8.

*** Note:** You must enable the access control list on which you want to set a rule. Only one access control list can be enabled at a time.

The command syntax is:

## Standard ACL

Avaya(configure)#access-list <*access-list-name*> <*access-list-index*> {permit [{use-priority <*priority*> | use-diffserv [mask] | remark-diffserv <*dscp*> [mask] | use-l2}] | deny | fwd1 | fwd2 | fwd3 | fwd4 | fwd5 | fwd6 | fwd7 | fwd8} {<*source-ip-addr*> <*source-wildcard*> | any | host <*source-ip-addr*>}

## Extended ACL

Avaya(configure)#access-list <*access-list-name*> <*access-list-index*> {permit [{use-priority <*priority*> | use-diffserv [mask] | remark-diffserv <*dscp*> [mask] | use-l2}] | deny | fwd1 | fwd2 | fwd3 | fwd4 | fwd5 | fwd6 | fwd7 | fwd8} <*protocol-id*> {<*source-ip-addr*>

<*source-wildcard*> | any | host <*source-ip-addr*>} [{lt <*port*> | eq <*port*> | gt <*port*> | range <*port*> <*port*>}] {<*dest-ip-addr*> <*dest-wildcard*> | any | host <*dest-ip-addr*>} [{lt <*port*> | eq <*port*> | gt <*port*> | range <*port*> <*port*>}] [established]

## Keywords, Arguments, and Options

***Table 6-150. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*access-list-name*> | A unique name that identifies the access control list. |
| <*access-list-index*> | The unique rule number within the access list. |
| permit | Forwards the packet without changing its priority. |
| use-priority | Assigns the priority that you define in the following <*priority*> parameter to the packet. |
| <*priority*> | The priority that you want to assign to packets that match this ACL. Enter a number between 0 and 7. |
| use-diffserv | Classifies traffic by the DSCP in the packet. |
| [mask] | Masks the three least significant bits of the DSCP.<br>If you mask the three least significant bits of the DSCP, the switch recognizes the remaining bits as the precedence field of the type of service (TOS) field and classifies the packets accordingly. |
| remark-diffserv | Replaces the DSCP in the packet with the DSCP that you enter for the following <*dscp*> parameter.<br>The switch uses the DSCP that you enter for the <*dscp*> parameter to classify the packet. |
| <*dscp*> | The DSCP that you want to replace the DSCP of the packet. |
| | ***1 of 3*** |

*Table 6-150. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| use-l2 | Classifies traffic by the layer 2 priority of the packet. If you enter **use-l2**, the switch ignores the ACL rule priority and DiffServ priority. |
| deny | Blocks the packet. |
| fwd1 \| fwd2 \| fwd3 \| fwd4 \| fwd5 \| fwd6 \| fwd7 \| fwd8 | The priority that you want to set.<br>The number following the **fwd** specifies the priority. The **fwd*x*** arguments are 1-based, while the queue priorities are 0-based. Consequently, the 1-based priorities are converted to 0-based priorities by the QoS features. For example, to specify a priority of 0, enter **fwd1**.<br>These keywords are retained from earlier versions of software for backward compatibility. The **use-priority <*priority*>** keyword and argument serve the same function. |
| <*protocol-id*> | The ID of the protocol that you want to assign a priority to. RFC791 defines the protocol IDs. |
| <*source-ip-addr*> | The source IP address of the subnet that you want to assign a priority to. |
| <*source-wildcard*> | The inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask.<br>This parameter specifies a range of IP address. For example, to specify all IP addresses in the 10.10.70 subnet, enter **10.10.70.0 0.0.0.255**. |
| any | A source of 0.0.0.0 and a source-wildcard of 255.255.255.255 |
| host <*source-ip-addr*> | The source IP address that you want to assign a priority to. |
| | ***2 of 3*** |

*Table 6-150. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| [{lt <*port*> \| eq <*port*> \| gt <*port*> \| range <*port*> <*port*>}] | A source port or range of source ports that pass between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). |
| <*dest-ip-addr*> | The destination IP address of the subnet that you want to assign a priority to. |
| <*dest-wildcard*> | The inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask.<br>This parameter specifies a range of IP address. For example, to specify all IP addresses in the 10.10.70 subnet, enter **10.10.70.0 0.0.0.255**. |
| any | A destination of 0.0.0.0 and a destination-wildcard of 255.255.255.255 |
| host <*dest-ip-addr*> | The destination IP address that you want to assign a priority to. |
| [{lt <*port*> \| eq <*port*> \| gt <*port*> \| range <*port*> <*port*>}] | A destination port or range of destination ports that pass data between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). |
| [established] | Permits TCP connections to be established that match the rule. |
| | ***3 of 3*** |

*** Note:** You must use the CLI to set up ACLs for QoS. Do not attempt to use the IP Access Control Web page in the Web Agent to set up ACLs for QoS.

## Examples: Standard ACL Rules

*Table 6-151. Examples: Standard ACL Rules*

| To . . . | Enter . . . |
|---|---|
| • Use the DSCP in the packet to classify all traffic that has a source IP address in the 10.10.60 subnet.<br>• Mask the three least significant bits of the DSCP. | **access-list MyAccessList1 4 permit use-diffserv mask 10.10.60.0 0.0.0.255** |
| Assign a priority of 7 to all traffic that has a source IP address in the 10.10.70 subnet. | **access-list MyAccessList1 5 permit use-priority 7 10.10.70.0 0.0.0.255** |
| • Replace the existing DSCP with a DSCP of 5 for all traffic that has a source IP address in the 10.10.80 subnet.<br>• Mask the three least significant bits of the DSCP | **access-list MyAccessList1 6 permit remark-diffserv 5 mask 10.10.80.0 0.0.0.255** |
| Use the layer 2 priority of the packet to classify all traffic that has a source address in the 11.11.11 subnet | **access-list MyAccessList1 7 permit use-l2 11.11.11.0 0.0.0.255** |
| Use the DSCP in the packet to classify all traffic that has a source IP address of 199.93.239.168 | **access-list MyAccessList1 8 permit use-diffserv host 199.93.239.168** |
| • Use the DSCP in the packet to classify all traffic that has a source IP address of 3.3.3.3<br>• Mask the three least significant bits of the DSCP | **access-list MyAccessList1 9 permit use-diffserv mask host 3.3.3.3** |
| Assign a priority of 2 to all traffic that has a source IP address of 1.1.1.1 | **access-list MyAccessList1 10 permit use-priority 2 1.1.1.1** |
| Block all traffic that has a source IP address of 10.1.0.55 | **access-list MyAccessList1 11 deny 10.1.0.55** |
| | |

## Examples: Extended ACL Rules

*Table 6-152. Examples: Extended ACL Rules*

| To . . . | Enter . . . |
|---|---|
| Use the DSCP in the packet to classify all traffic that has a:<br>• Source IP address of 199.93.239.168<br>• Destination address in the 1.1.1 subnet | **access-list MyAcessList2 1 permit use-diffserv ip host 199.93.239.168 1.1.1.0 0.0.0.255** |
| Use the DSCP in the packet to classify all traffic that has a:<br>• Source IP address in the 3.0 subnet<br>• Destination address in the 5.0 subnet<br>• Mask the three least significant bits of the DSCP | **access-list MyAccessList2 2 permit use-diffserv mask ip 3.0.0.0 0.255.255.255 5.0.0.0 0.255.255.255** |
| Assign a priority of 2 to all TCP traffic that has a:<br>• Source IP address in the 1.1 subnet<br>• Source port that is greater than 24<br>• Destination IP address in the 6.6 subnet<br>• Destination port of 23 | **access-list MyAccessList2 3 permit use-priority 2 tcp 1.1.0.0 0.0.255.255 gt 24 6.6.0.0 0.0.255.255 eq 23** |
| • Replace the existing DSCP of packets with a DSCP of 12 for all traffic that has a source IP address of 199.93.238.83.<br>• Mask the three least significant bits of the DSCP. | **access-list MyAccessList2 4 permit remark l2 mask ip host 199.93.238.83 any** |
| Replace the existing DSCP of the packet with a DSCP of 24 for all ICMP traffic that has a:<br>• Source IP address of 2.2.2.2<br>• Destination IP address of 4.4.4.4 | **access-list MyAccessList2 5 permit remark 24 icmp host 2.2.2.2 host 4.4.4.4** |
| | ***1 of 2*** |

*Table 6-152. Examples: Extended ACL Rules*

| To . . . | Enter . . . |
|---|---|
| Assign a priority of 6 to all TCP traffic that has a:<br>• Source IP address in the 10.10.10 subnet<br>• Destination IP address in the 11.11.11 subnet<br>• Destination port of 1 | **access-list MyAccessList2 6 permit use-priority 6 tcp 10.10.10.0 0.0.0.255 11.11.11.0 0.0.0.255 eq 1** |
| Use the layer 2 priority in the packet to classify all UDP traffic | **access-list MyAccessList2 7 permit use-l2 udp any any** |
| • Use the layer 2 priority in the packet to classify all TCP traffic that has a:<br>— Source IP address in the 5.5.5 subnet<br>— Destination IP address in the 6.6.6 subnet<br>— Destination port that is less than 2<br>• Permit TCP connections that meet this criteria | **access-list MyAccessList2 8 permit use-l2 tcp 5.5.5.0 0.0.0.255 6.6.6.0 0.0.0.255 lt 2 established** |
| • Use the DSCP to classify all UDP traffic that has a:<br>— Source IP address of 7.7.7.7<br>— Destination IP address of 8.8.8.8<br>— Destination port between 33 and 44<br>• Mask the three least significant bits of the DSCP | **access-list MyAccessList2 9 permit use-diffserv mask udp host 7.7.7.7 host 8.8.8.8 range 33 44** |
| • Assign a priority of 7 to all TCP traffic that has a:<br>— Source IP address of 9.9.9.9<br>— Destination IP address of 3.3.3.3<br>— Destination port between 55 and 66<br>• Permit TCP connections that meet this criteria | **access-list MyAccessList2 10 permit use-priority 7 tcp host 9.9.9.9 host 3.3.3.3 range 55 66 established** |
| | ***2 of 2*** |

# Setting Up a Default ACL Rule

## Command

Use the **any** keyword in the **access list** command to set up a default ACL rule. The rule will be applied to all packets on the switch that do match any other ACL rules. The command syntax is:

Avaya(configure)#access-list <*access-list-name*> <*access-list-index*> {permit [{use-priority <*priority*> | use-diffserv [mask] | remark-diffserv <*dscp*> [mask] | use-l2}] | fwd1 | fwd2 | fwd3 | fwd4 | fwd5 | fwd6 | fwd7 | fwd8} any

The default ACL rule must have the highest index in the ACL. To ensure that the switch never applies the default ACL rule to traffic that matches other ACL rules, Avaya recommends that you use an index of 512 for the default ACL rule.

For more information about how default ACL rules work, see "Classifying Traffic by Layer 3 or Layer 4 Characteristics" on page 8.

## Examples

***Table 6-153. Default ACL Rules***

| To . . . | Enter . . . |
|---|---|
| Use the DSCP in the packet to classify all traffic that does not match any other ACL rule. | **access-list MyAcessList1 512 permit use-diffserv any** |
| Replace the existing DSCP with a DSCP of 63 for all traffic that does not match any other ACL rule.<br>The switch uses the new DSCP of 63 to classify the packets. | **access-list MyAcessList1 512 permit remark-diffserv 63 any** |
| Use the layer 2 priority in the packet to classify all traffic that does not match any other ACL rule. | **access-list MyAcessList1 512 permit use-l2 any** |
| Assign a priority of 4 to all traffic that does not match any other ACL rule. | **access-list MyAcessList1 512 permit use-priority 4 any** |
| | |

## Displaying ACL Rules

### Command

Use the **show access-lists** command to display the ACL rules in an ACL.

The syntax of this command is:

Avaya>show access-lists [<*access-list-name*>]

For more information on this command, see Chapter 18, "Policy," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*.

# Ingress Policing

Policing makes it possible for you to limit the bandwidth for ingress queues. You limit the bandwidth by specifying the guaranteed bit rate for a port. If this bit rate is exceeded, the switch drops the excess packets.

For example, if you set policing on an ingress queue to be 5 Mbps, and traffic exceeds that 5 Mbps rate, all traffic that exceeds the 5Mbps is dropped.

Only 80-series modules that are licensed for routing support the policing feature.

The policing algorithm includes a normal burst threshold. This threshold sets the size of bursts that is guaranteed transfer.

The switch uses queue 7 to forward protocol packets (ARP, VRRP, OSPF, and so on) to the supervisor module. Do not disable this queue. If you disable it, all protocol packets and learned packets are discarded before reaching the supervisor module. If you enable policing on queue 7, be sure to allocate the queue enough bandwidth for management packets and learned packets. Failure to allocate enough bandwidth to the queue may result in poor network performance.

For information about how to set up policing, see "Setting Up Policing" on page 32.

*** Note:** Avaya recommends that you do not set a port using policing as the source port or mirror port for a port mirror. When the switch limits the bandwidth of a port, packets are subject to random drop. If packets from a

source port or mirror port are dropped, the mirror traffic may not match the source traffic.

## Setting Up Policing

Use the **set port police** command to enable or disable policing for ingress traffic on a port. For information on how policing works, see "Ingress Policing" on page 31.

The syntax for this command is:

Avaya <configure># set port police {{<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] | all-ports} queue <*queue*> {bit-rate <*rate*> normal-burst <*normal-burst*> | disable}

***Table 6-154. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, policing is enabled for all ports on the module in the slot that you specify. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, policing is enabled for the port or range of ports on the module in the slot that you specify. |
| all-ports | All ports in the chassis. If you specify **all-ports**, policing is enabled on all modules in the chassis. |
| <*queue*> | The queue number, which can range from 0 to 7. |
| | ***1 of 2*** |

*Table 6-154. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*rate*> | The maximum bits per second that you want to assign to the queue.<br>For Fabric mode 1, enter:<br>• 0 to disable the queue<br>**Or**<br>• 220 Kbps to 1.5 Gbps<br>For Fabric mode 2, enter:<br>• 0 to disable the queue<br>**Or**<br>• 270 Kbps to 1.5 Gbps |
| <*normal-burst*> | This threshold sets the maximum size of burst that is guaranteed transfer.<br>The normal burst can range from 0 to 15,000. Avaya recommends a setting of 4. |
| disable | Disables policing. |
| | ***2 of 2*** |

# Displaying the Policing Settings

Use the **show port police** command to display the settings for policing. For information on how policing works, see "Ingress Policing" on page 31.

The syntax for this command is:

Avaya>show port police {<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}]

***Table 6-155. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, the switch displays the policing settings for all ports on the module in the slot that you specify. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the switch displays the policing settings for the port or range of ports on the module in the slot that you specify. |
| | |

# Queue-Servicing Algorithms

The following queue-servicing algorithms are available for egress queues:

- Weighted fair queueing (WFQ)
- Strict Priority
- Class-based queueing (CBQ)
- Class-based weighted fair queueing (CBWFQ)

*** Note:** In earlier versions of the switch software, you could set ingress queues to use the weighted fair queuing (WFQ) and strict priority queue-servicing algorithms. In v5.3.1, you can set only egress queues to use these queue-servicing algorithms. To service ingress queues, use the policing feature.

## WFQ

### How WFQ Works

WFQ is the default queue-servicing algorithm. When a port is set to use the WFQ algorithm, each queue:

- Is assigned a weight increment. This value never changes.
- Maintains an accumulated weight. After the switch services a queue, its accumulated weight is reset to the value of its weight increment, and the accumulated weight for the other queues is increased by their respective weight increments.

The switch always services the queue that has the highest *accumulated weight*. If two queues have the same accumulated weight, the switch first services the queue that has the highest priority (0 – 7).

Table 6-156 lists the default weight increment for each queue.

***Table 6-156. Default Weight Increments***

| Queue | Weight Increment |
|---|---|
| WFQ 0 | 1 |
| WFQ 1 | 2 |
| WFQ 2 | 4 |
| | ***1 of 2*** |

*Table 6-156. Default Weight Increments*

| Queue | Weight Increment |
|---|---|
| WFQ 3 | 8 |
| WFQ 4 | 16 |
| WFQ 5 | 32 |
| WFQ 6 | 64 |
| WFQ 7 | 128 |
| | *2 of 2* |

For information on how to set up WFQ, see "Setting Up WFQ" on page 39.

### Example

Suppose that the accumulated weight of all queues is set at their weight increments.

1. The switch services queue 7 because its accumulated weight is 128.
2. The accumulated weight of queue 7 is reset to 128, and the accumulated weight of all other queues is increased by their weight increment.

   At this point, queue 7 and queue 6 both have an accumulated weight of 128.
3. The switch services queue 7 because it is the higher priority queue.
4. The accumulated weight of queue 7 is then reset to 128, and the accumulated weight of all other queues is increased by their weight increment.

   Now queue 6 has an accumulated weight of 192, and queue 7 has an accumulated weight of 128.
5. The switch services queue 6 because it has the higher accumulated weight.

## Strict Priority Queueing

With strict priority queuing, the switch services the eight queues in order of their priority. The highest priority queue is serviced until it is empty, and then the lower priority queues are serviced sequentially until they are empty. For example, queue 7 must be empty before the switch services queue 6. Queue 6 must be empty

before the switch services queue 5. Queue 5 must be empty before the switch services queue 4, and so on.

For information on how to set up strict priority queueing, see "Setting Up Strict Priority Queueing" on page 40.

## CBQ

With the class-based queuing (CBQ) algorithm, you can specify a maximum bit rate, or bandwidth, for a queue. When that bit rate is exceeded, the switch drops all packets that exceed the bit rate.

The bit rate that you set should be the long-term average rate of transmission. Traffic that does not exceed this rate is guaranteed transfer.

For information on how to set up CBQ queueing, see "Setting Up CBQ" on page 41.

*** Note:** Avaya recommends that you do not set a port using CBQ as the source port or mirror port for a port mirror. When the switch limits the bandwidth of a port, packets are subject to random drop. If packets from a source port or mirror port are dropped, the mirror traffic may not match the source traffic.

## CBWFQ

The class-based weighted fair queueing (CBWFQ) algorithm is a combination of the CBQ and WFQ algorithms. CBWFQ makes more complex management of traffic possible. Using CBWFQ, you can set:

- The maximum bit rate.

  The bit rate that you set should be the long-term average rate of transmission. Traffic that does not exceed this rate is guaranteed transfer.

- Burst thresholds
- The action that you want the switch to take when the bit rate exceeds the maximum bit rate.

  — Drop the packets

  **Or**

  — Forward the packets according to the weight of the queue

*** Note:** Avaya recommends that you do not set a port using CBWFQ as the source port or mirror port for a port mirror. When the switch limits the bandwidth of a port, packets are subject to random drop. If packets from a source port or mirror port are dropped, the mirror traffic may not match the source traffic.

### Burst Thresholds

The CBWFQ algorithm has two burst thresholds that you can set. Both of thresholds are set in a number of bytes.

- Normal burst—This threshold sets the maximum size burst that is guaranteed transfer. Bursts that are smaller than this size are guaranteed transfer. Bursts that are larger than this size are either serviced by WFQ or dropped (whichever action that you specify). The default setting is servicing by WFQ and the default weight for the queues. Normal burst size can range from 0 to 15,000 bytes.
- Maximum burst—This threshold sets the maximum size burst that is serviced by WFQ once the normal burst has been exceeded. Bursts that are smaller than this size are serviced by WFQ. Bursts that are larger than this size are dropped. If you set this threshold to the same value as normal burst, the maximum burst capability is disabled. The maximum burst can range from the normal burst size to 15,000.

## Management Traffic

The switch uses the following priority queues to forward protocol packets (ARP, VRRP, OSPF, and so on) from the supervisor module:

- On switches with an 80-series supervisor module, queue 7.
- On switches with a Layer 3 supervisor module, queue 4.

Do not disable these queues. If you disable these queues, all protocol packets are discarded. If you enable shaping on these queues, be sure to allocate the queues enough bandwidth for management packets. Failure to allocate enough bandwidth to the queue may result in poor network performance.

# Setting Up WFQ

Use the **set port queue service wfq** command to set a port, port range, or module to use weighted fair queueing (WFQ) queue servicing. WFQ is the default queue-servicing algorithm.

The syntax of the command is:

Avaya(configure)#set port queue service {{<*mod-num*> | <*mod-swport-range*>} [...,{<*mod-num*> | <*mod-swport-range*>}] | all-ports} wfq {queue <*queue*> weight <*weight*> | default}

***Table 6-157. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, all ports on the module are set to use WFQ. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the port or range of ports that you specify is set to use WFQ. |
| all-ports | All ports in the chassis. If you specify **all-ports**, all ports on all modules in the chassis are set to use WQF. |
| <*queue*> | The queue number, which can range from 0 to 7. |
| <*weight*> | The weight that you want to assign to the queue. Weights can range from 1 to 254. |
| default | The default weights. For the specific default weight of each queue, see Table 6-156 on page 21-35. |
| | |

For information about how WFQ works, see "WFQ" on page 35.

# Setting Up Strict Priority Queueing

## Command

Use the **set port queue service strict-priority** command to set a port, port range, or module to use strict priority queue servicing.

The syntax of the command is:

Avaya(configure)#set port queue service {{<*mod-num*> | <*mod-swport-range*>} [...,{<*mod-num*> | <*mod-swport-range*>}] | all-ports} strict-priority

***Table 6-158. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, all ports on the module are set to use strict priority queueing. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the port or range of ports on the module that you specify is set to use strict priority queueing. |
| all-ports | All ports in the chassis. If you specify **all-ports**, all ports on all modules in the chassis are set to use strict priority queueing. |
| | |

For information on how strict priority queueing works, see "Strict Priority Queueing" on page 36.

## Example

To set ports 1 through 12 on module 5 to use strict priority queueing, enter:

**set port queue service 5/1-12 strict-priority**

# Setting Up CBQ

Use the **set port queue service cbq** command to set a port, port range, or module to use class-based queuing (CBQ) queue servicing. The syntax of the command is:

Avaya(configure)# set port queue service {{<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] | all-ports} cbq queue <*queue*> bit-rate <*rate*>

***Table 6-159. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, all ports on the module are set to use CBQ. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the port or range of ports that you specify is set use CBQ. |
| all-ports | All ports in the chassis. If you specify **all-ports**, all ports on all modules in the chassis are set to use CBQ. |
| <*queue*> | The queue number, which can range from 0 to 7. |
| | ***1 of 2*** |

*Table 6-159. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*rate*> | The maximum bits per second that you want to assign to the queue.<br>If the switch is operating in *Fabric mode 1*, the rate can range from 220 Kbps to 1.5 Gbps.<br>If the switch is operating in *Fabric mode 2*, the rate can range from 270 Kbps to 1.5 Gbps<br>Entering a rate of 0 disables the queue. |
| | ***2 of 2*** |

For information about how the CBQ queue-servicing algorithm works, see "CBQ" on page 37.

## Setting Up CBWFQ

Use the **set port queue service cbwfq** command to set a port, port range, or module to use class-based weighted fair queuing (CBWFQ) queue servicing. The syntax of the command is:

Avaya(configure)# set port queue service {{<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] | all-ports} cbwfq queue <*queue*> bit-rate <*rate*> normal-burst <*normal-burst*> [exceed {drop | max-burst <*max-burst*> [weight <*weight*>]}]

*Table 6-160. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, all ports on the module are set to use CBQ. |
| | ***1 of 4*** |

*Table 6-160. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the port or range of ports that you specify is set use CBQ. |
| all-ports | All ports in the chassis. If you specify **all-ports**, all ports on all modules in the chassis are set to use CBQ. |
| <*queue*> | The queue number, which can range from 0 to 7. |
| <*rate*> | The maximum bits per second that you want to assign to the queue.<br>If the switch is operating in *Fabric mode 1*, the rate can range from 220 Kbps to 1.5 Gbps.<br>If the switch is operating in *Fabric mode 2*, the rate can range from 270 Kbps to 1.5 Gbps<br>Entering a rate of 0 disables the queue. |
| | ***2 of 4*** |

*Table 6-160. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*normal-burst*> | The maximum size of burst that is guaranteed transfer. Bursts that are smaller than this size are guaranteed transfer. Bursts that are larger than this size are either serviced by WFQ or dropped (whichever action that you specify). The default setting is servicing by WFQ and the default weight for the queues.<br>The normal burst can range from 0 to 15,000 bytes. Avaya recommends a value of 6000.<br>Enter this setting in a multiple of four. If you do not enter a multiple of four, the switch rounds down the number that you enter to a multiple of four. For example, if you enter a normal burst size of 43 byes, the switch converts the setting to 40 bytes. If you enter a normal burst size of 0,1,2 or 3, the switch stores a value of 0 and no data is forwarded from the queue. |
| exceed | The action that you want the switch to take if the bit rate exceeds the guaranteed bit rate that you specify. The switch can either drop packets or forward them based on the weight of the queue. |
| drop | Indicates that you want the switch to drop packets when the bit rate exceeds the guaranteed bit rate. |
| | ***3 of 4*** |

*Table 6-160. Keywords, Arguments, and Options*

| Keyword, Argument or Option | Definition |
|---|---|
| <*max-burst*> | The maximum size burst that is serviced by WFQ once the normal burst has been exceeded. Bursts that are smaller than this size are serviced by WFQ. Bursts that are larger than this size are dropped. If you set this threshold to the same value as normal burst, the maximum burst capability is disabled.<br>The maximum burst can range from the normal burst size to 15,000.Avaya recommends a value of 6000.<br>Increase the maximum burst setting as the burstiness of the traffic increases.<br>**Note:** The maximum burst setting must be greater than or equal to the normal burst.<br>Enter this setting in a multiple of four. If you do not enter a multiple of four, the switch rounds down the number that you enter to a multiple of four. For example, if you enter a maximum burst size of 43 byes, the switch converts the setting to 40 bytes.If you enter a maximum burst size of 0,1,2 or 3, the switch stores a value of 0 and no data is forwarded from the queue. |
| <*weight*> | The weight that you want to assign to the queue. Weights can range from 1to 254. |
| | ***4 of 4*** |

For information about how CBWFQ works, see "CBWFQ" on page 37.

*** Note:** The switch does not drop packets on egress queue 7, even if you specify the **drop** keyword. This restriction ensures that traffic management packets are not discarded by the bandwidth-limiting functions. In spite of the ability of egress queue 7 to exceed its bandwidth limit, the queue is subject to a fairness mechanism that prevents other queues (6 through 0) from being starved. Note that, when you specify **drop**, the bandwidth of queue 7 is limited if lower priority queues require service and have not reached their bandwidth guarantee.

# Displaying the Queue-Service Settings

## Command

Use the **show port queue service** command to display the settings for queue servicing. The syntax for this command is:

Avaya>show port queue service {<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}]

***Table 6-161. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, the switch displays queue-service settings for all ports on the module in the slot that you specify. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the switch displays the queue-service settings for the port or range of ports that you specify. |
| | |

## Example

To display the queue service settings for port 1 on the module in slot 3, enter:

**show port queue service 3/1**

# QoS Statistics

You can display QoS statistics for:

- All ports on a module
- A port or port range
- A specific queue on a port, port range, or module

Two sets of statistics are displayed for egress queues: port statistics and queue statistics. For ingress queues, only queue statistics are displayed.

Table 6-162 lists the statistics that are displayed for ingress queues. Table 6-164 lists the statistics that are displayed for egress ports. And Table 6-165 lists the statistics that are displayed for egress queues.

For information on how to display the QoS Statistics, see "Displaying QoS Statistics".

## Queue Statistics

Table 6-162 lists the statistics that the switch displays for ingress and egress queues.

***Table 6-162. Ingress Queue Statistics for 10/100 Modules***

| Statistic | Explanation |
|---|---|
| Frames Dropped Queue Full | The total number of frames that were dropped because the queue was full. This number is cumulative since the last reset of the statistics. |
| Frames Enqueued | The total number of frames stored in the queue. This number is cumulative since the last reset of the statistics. |
| | ***1 of 3*** |

*Table 6-162. Ingress Queue Statistics for 10/100 Modules*

| Statistic | Explanation |
|---|---|
| Threshold (% Full) | The threshold for queue capacity that determines whether additional frames are counted toward **Frames Enqueued Above Threshold** or **Frames Enqueued Below Threshold**.<br>If the number of frames in the queue exceeds this percentage of the queue capacity, the **Frames Enqueued Above Threshold** count is increased when another frame is added to the queue.<br>If the number of frames in the queue does *not* exceed this percentage of the queue capacity, the **Frames Enqueued Below Threshold** count is increased when another frame is added to the queue. |
| Frames Enqueued Above Threshold | The total number of frames that were added to the queue when the number of frames in the queue exceeded the **Threshold (% Full)**. This number is cumulative since the last reset of the statistics. |
| Frames Enqueued Below Threshold | The total number of frames that were added to the queue when the number of frames in the queue did *not* exceed the **Threshold (% Full)**. This number is cumulative since the last reset of the statistics. |
| Peak Size (% Full) | The highest percentage of queue capacity that the queue has reached since the last reset of the statistics. |
| Frames Dropped Age Out | The total number of frames that have aged out of the queue (dropped from the queue). This number is cumulative since the last reset of the statistics. |
| | ***2 of 3*** |

*Table 6-162. Ingress Queue Statistics for 10/100 Modules*

| Statistic | Explanation |
|---|---|
| Frames Dequeued | The total number of frames that were removed from the queue and forwarded to the egress physical port for transmission. This number is cumulative since the last reset of the statistics.<br>The total number of frames that were forwarded from the queue.<br>The total number of frames that were removed from the queue and |
| Bytes Dequeued | The total number of bytes that were removed from the queue and forwarded to the egress physical port for transmission. This number is cumulative since the last reset of the statistics. |
| | *3 of 3* |

## Egress Port Statistics for 10/100 Modules

The egress port statistics for 10/100 modules are reported per 12 ports, not for individual physical ports. For example, if you display the QoS statistics for port 20 on a 10/100 module, the port statistics that are displayed reflect the cumulative statistics of ports 13 through 24, not for just port 20.

Table 6-163 lists the port ranges for which egress port statistics are reported on 10/100 modules.

*Table 6-163. Port Ranges for 10/100 Egress Port Statistics*

| Module | Port Ranges for which Port Statistics Are Reported |
|---|---|
| 24-port 10/100 modules | • 1 set of statistics for ports 1–12.<br>• 1 set of statistics for ports 13–24. |
| 48-port 10/100 modules | • 1 set of statistics for ports 1–12.<br>• 1 set of statistics for ports 13–24.<br>• 1 set of statistics for ports 25–36<br>• 1 set of statistics for ports 37–48 |
| | |

Table 6-164 lists the statistics that the switch displays for ports on 10/100 modules.

***Table 6-164. Egress Port Statistics for 10/100 Modules***

| Statistic | Explanation |
|---|---|
| Frames Arriving Switch Fabric | The number of frames that the module received from the switch fabric. This number is cumulative since the last reset of the statistics. |
| Frames Dropped Runt | The number of frames that the port range dropped because they were smaller than the minimum frame size of 60 bytes. This number is cumulative since the last reset of the statistics. |
| Frames Dropped Parity Error | The number of frames that the port range dropped because they had a parity error. This number is cumulative since the last reset of the statistics. |
| Frames Dropped Flood Rate Limit | The number of frames that the port range dropped due to flood rate limiting. This number is cumulative since the last reset of the statistics. |
| | |

## Egress Port Statistics for Gigabit Modules

The egress port statistics for gigabit modules are reported per individual port. Table 6-165 lists the statistics that the switch displays for ports on gigabit modules.

***Table 6-165. Egress Port Statistics for Gigabit Modules***

| Statistic | Explanation |
|---|---|
| Frames Arriving Switch Fabric | The number of frames that the module received from the switch fabric. This number is cumulative since the last reset of the statistics. |
| Unicast Frames Enqueued | The number of unicast frames that the port queued. This number is cumulative since the last reset of the statistics. |
| Unicast Bytes Enqueued | The number of unicast bytes that the port queued. This number is cumulative since the last reset of the statistics. |
| Multicast Frames Enqueued | The number of multicast frames that the port queued. This number is cumulative since the last reset of the statistics. |
| | ***1 of 2*** |

*Table 6-165. Egress Port Statistics for Gigabit Modules*

| Statistic | Explanation |
|---|---|
| Multicast Bytes Enqueued | The number of multicast bytes that the port queued. This number is cumulative since the last reset of the statistics. |
| Broadcast Frames Enqueued | The number of broadcast frames that the port queued. This number is cumulative since the last reset of the statistics. |
| Broadcast Bytes Enqueued | The number of broadcast bytes that the port queued. This number is cumulative since the last reset of the statistics. |
| Frames Dropped Runt | The number of frames that the port dropped because they were smaller than the minimum frame size of 60 bytes. This number is cumulative since the last reset of the statistics. |
| Frames Dropped Parity Error | The number of frames that the port dropped because they had a parity error. This number is cumulative since the last reset of the statistics. |
| Frames Dropped Huge (> 24KBytes) | The number of frames that the port dropped because they were larger than 24,000 bytes. This number is cumulative since the last reset of the statistics. |
| Frames Dropped Keep Logic | The number of frames that the port dropped because of parity errors, frame sizes less than 60 bytes, flood rate limiting, a queue being full, and frame sizes larger than 24,000 bytes. This number is cumulative since the last reset of the statistics. |
| Frames Dropped Packet Memory Full | The number of frames that the port dropped because the queue memory was full. This number is cumulative since the last reset of the statistics. |
| Frames Forwarded to MAC | The number of frames that were removed from the queue and forwarded to the MAC address. This number is cumulative since the last reset of the statistics. |
| | ***2 of 2*** |

## Buffer Statistics for Egress Queues

You can also display the amount of memory that is allocated to each egress queue. The allocated amount of memory is displayed in both the number of buffers and the number of bytes. Buffers are 128-byte units of memory that store packets in the queues.

Table 6-166 lists the buffer statistics that you can display for egress queues. These settings are determined by the switch. You can display them but not change them.

***Table 6-166. Buffer Statistics for Egress Queues***

| Statistic | Explanation |
|---|---|
| Total Queue Memory (buffers) | The total number of buffers that are allocated to all queues on the port. |
| Total Queue Memory (bytes) | The total number of bytes that are allocated to all queues on the port. |
| Age Out Interval | The maximum number of milliseconds that a queue can store a packet. If the switch does not forward the packet before this time period expires, the queue drops the packet. |
| Reserved Allocation (buffers) | The number of buffers that are allocated to a specific queue. These buffers are dedicated to the queue and cannot be used by another queue. |
| Reserved Allocation (bytes) | The number of bytes that are allocated to a specific queue. These bytes are dedicated to the queue and cannot be used by another queue. |
| Maximum Allocation (buffers) | The maximum number of buffers that can be allocated to a specific queue if extra buffers are available (not being used by another queue). |
| Maximum Allocation (bytes) | The maximum number of bytes that can be allocated to a specific queue if extra bytes are available (not being used by another queue). |
| Minimum Free Pool After Allocation (buffers) | The minimum number of empty buffers that the port must have available at all times.<br>If queues exceed their **Reserved Allocation**, they can consume buffers in their **Maximum Allocation** only until the pool of empty buffers reaches this number. |
| | |

# Displaying QoS Statistics

Use the **show port queue counters** to display QoS statistics. The syntax of this command is:

Avaya> show port queue counters {<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] {ingress | egress | all} [queue <*queue*>]

***Table 6-167. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, the switch displays the QoS statistics for all ports on the module that you specify. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the switch displays the QoS statistics for the port or range of ports that you specify. |
| {ingress \| egress \| all} | The direction of traffic that you want to view the Qos Statistics for.<br>• Enter **ingress** to view the QoS statistics for ingress queues.<br>• Enter **egress** to view the QoS statistics for egress queues.<br>• Enter **all** to view the QoS statistics for both ingress and egress queues. |
| <*queue*> | The queue number, which can range from 0 to 7. If you do not specify a queue number, the switch displays all QoS statistics for the port or module. |
| | |

For more information about the QoS statistics, see "Setting the Priority of a Physical Port" on page 13

# Resetting the QoS Statistics

Use the **reset port queue counters** to reset the queue statistics to 0. The syntax of the command is:

Avaya> reset port queue counters {<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] {ingress | egress | all} [queue <*queue*>]

***Table 6-168. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, the switch resets the the QoS statistics for all ports on the module that you specify. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the switch resets the QoS statistics for the port or range of ports that you specify. |
| {ingress \| egress \| all} | The direction of traffic that you want to reset the QoS statistics for.<br>• Enter **ingress** to view the QoS statistics for ingress queues.<br>• Enter **egress** to view the QoS statistics for egress queues.<br>• Enter **all** to view the QoS statistics for both ingress and egress queues. |
| <*queue*> | The queue number, which can range from 0 to 7. If you do not specify a queue number, the switch resets the QoS statistics for all queues on the port. |
| | |

# Displaying the Buffer Settings for Egress Queues

Use the **show port queue buffer** command to display the amount of memory that is assigned to each queue.

The syntax of the command is:

Avaya (configure)#show port queue buffer {{<*mod-num*> | <*mod-swport-range*>} [..., {<*mod-num*> | <*mod-swport-range*>}] | all-ports}

***Table 6-169. Keywords, Arguments, and Options***

| Keyword, Argument or Option | Definition |
|---|---|
| <*mod-num*> | The slot number of a module. If you specify <*mod-num*>, the switch displays the number of packet buffers that are allocated to the egress queues on all ports on the module that you specify. |
| <*mod-swport-range*> | The slot number of a module, and, either a port number, or a range of port numbers having the format *Px-Py*. For example:<br>• To specify port 1 on the module in slot 3, enter **3/1**.<br>• To specify ports 1 through 5 on the module in slot 3, enter **3/1-5**.<br>If you specify <*mod-swport-range*>, the switch displays the number of packet buffers that are allocated to the egress queues on the port or range of ports that you specify. |
| {all-ports} | All ports in the chassis. If you specify **all-ports**, the switch displays the number of packet buffers that are allocated to the egress queues on all ports in the chassis. |
| | |

# A Upgrading the Application Software

## Overview

Upgrading the switch software involves the following steps:

1. Backing Up the Current Software
2. Backing Up the Previous Configuration
3. Downloading Application Software
4. Setting the Startup Image
5. Synchronizing the Active and Standby Supervisor Modules
6. Resetting the Active Supervisor
7. Resetting the Standby Supervisor
8. Verifying the Upgrade

This appendix contains procedures for each of these steps.

If a redundant supervisor module is running a 4.*x* version of application software, it is not upgraded to v5.*x* if you follow this upgrade procedure. To upgrade the application software from v4.x to v5.*x* on a switch that has a redundant supervisor module, you must upgrade the application software on each supervisor module individually. For information on how to perform this task, see "Upgrading from v4.x to v5.x" on page A-10.

If the switch has multiple VLANs statically bound to hunt group ports, after upgrading from v5.*x* to v5.3.*x*, you must delete the hunt groups and set them up again. For information on how to perform this task, see "Upgrading a Switch with Multiple VLANs Statically Bound to Hunt Group Ports" on page A-11.

# Backing Up the Current Software

The Avaya Multiservice switches have two memory locations for storing the embedded switch software: APP1 and APP2. These two memory locations make it possible to store the current software in one APP location and download the new software to the other APP location.

Saving the current software in one APP location ensures that you could run this earlier version of software, if you encounter any problem with the new, downloaded software.

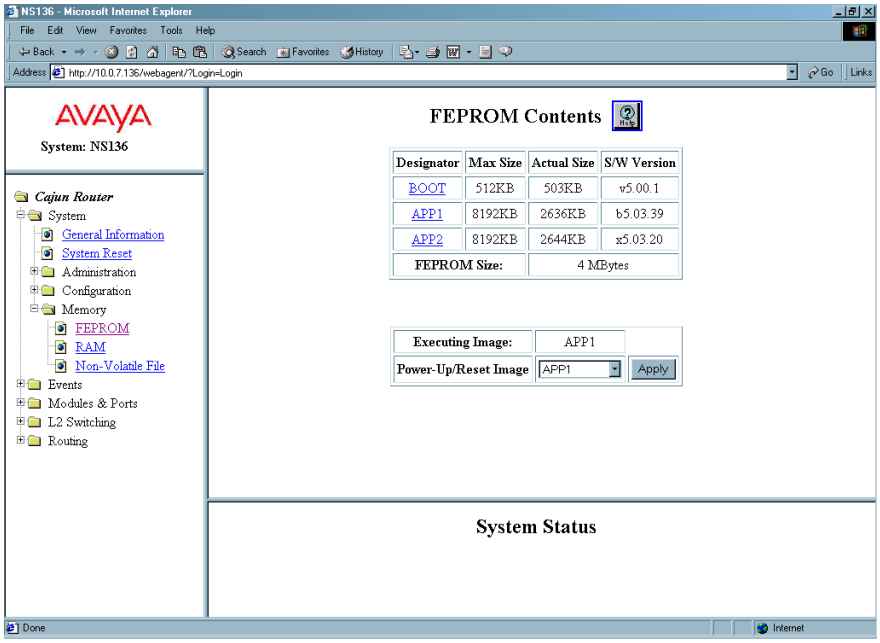
## Web Agent Procedure

To determine the APP location from which the switch loads the previous version of software:

1. In the navigation pane, expand the **System** > **Memory** folders.
2. Select **FEPROM**.

   The FEPROM Contents Web page is displayed in the content pane (Figure A-183). The **Power-Up/Reset Image** field displays the APP memory location from which the switch loads the switch software.

***Figure A-183. FEPROM Contents Web page***



3. When you download the new switch software, download it to the other APP memory location. For example, in Figure A-183, you would download the new software to APP2.

### CLI Command

To determine the APP location from which the switch loads the previous version of software, use the following command:

**Avaya>show flash**

This command displays information about the application software that is currently stored in APP1 and APP2. For more information about this command, see Chapter 27, "System," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches*.

# Backing Up the Previous Configuration

Before you upgrade the switch software it is advised that the previous configuration is backed up to a file or directory on a TFTP server, back up the previous configuration to a file or directory on a TFTP server. You can use either the Web Agent or CLI to perform this task.

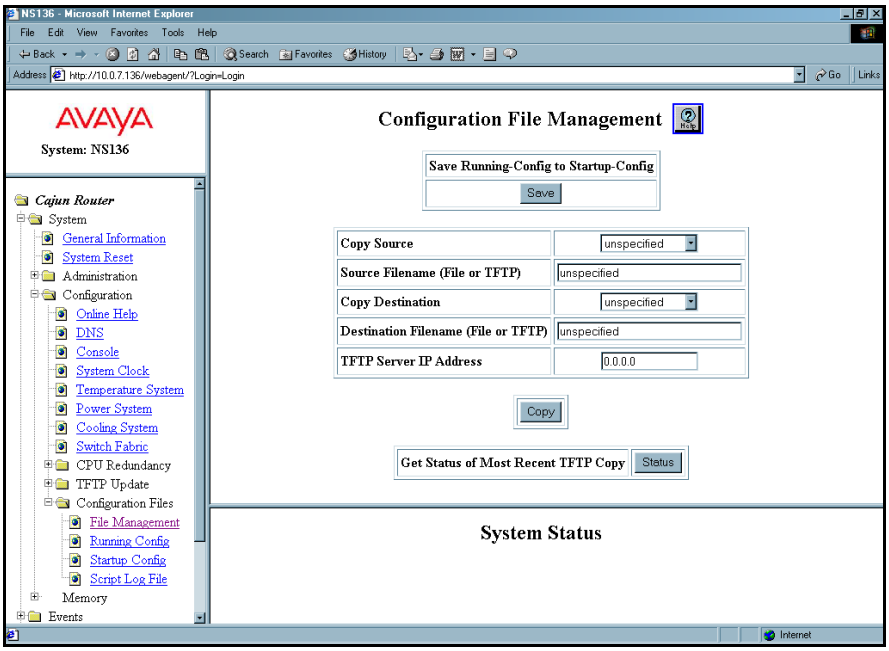
### Web Agent Procedure

To back up the previous configuration by using the Web Agent:

1. In the navigation pane, expand the **System** > **Configuration** > **Configuration Files** folders.
2. Select **File Management**.

   The **Configuration File Management** Web page is displayed in the content pane (Figure A-184).

*Figure A-184. Configuration File Management Web page*




3. In the **Save Running-Config to Startup-Config** field, select **Save**.

4. In the **Copy Source** field, select **Startup-Config**.

*** Note:** The Source File name may be left unspecified

5. In the **Copy Destination** field, select **TFTP Server**.

*** Note:** You must specify a Destination file name.

6. In the **TFTP Server IP Address** field, enter the IP address of the TFTP server to which you want to copy the startup configuration file.

7. Click **Copy**.

## CLI Command

To back up the current configuration to a TFTP server, use the following command:

**Avaya#copy tftp <*filename-opt-path*>**

For more information on this command, see Chapter 27, “System,” in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches.*

# Downloading Application Software

You can download new application software from a TFTP server to an APP memory location by using either the Web agent or the CLI.

## Web Agent Procedure

To download new application software from a TFTP server to an APP memory location by using the Web Agent:

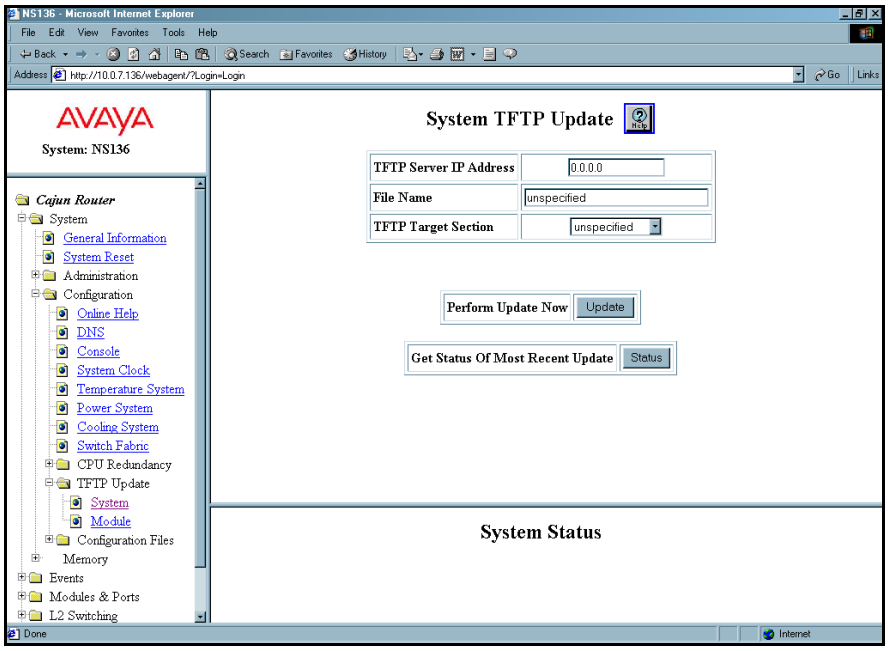
*** Note:** The switch does not support Exceed TFTP server software.

1. In the navigation pane, expand the **System** > **Configuration** > **TFTP Update** folders.
2. Select **System**.

   The **System TFTP Update** Web page is displayed in the content pane (Figure A-185).

*** Note:** Only boot code versions 5.00.01 and later are supported.

***Figure A-185. System TFTP Update Web page***




3. In the **TFTP Server IP Address** field, enter the IP address of the TFTP server on which the new application software is stored.

4. In the **File Name** field, enter one of the following:
   - **m5500r_v5.03.01.bin** to download version 5.3.1 for the P550R switch (layer 3)
   - **m8000r_v5.03.01.bin** to download version 5.3.1 for the P580 switch (layer 3)
   - **m8800_v5.03.01.bin** to download version 5.3.1 for the P880 switch
   - **m8000r_v5.03.01.bin** to download version 5.3.1 for the P882 switch
5. In the **TFTP Target Section** field, select the memory location to which you want to download the new application software.
6. In the **Perform Update Now** field, select **Update**.
7. In the **Get Status of Most Recent Update** field, select **Status** to verify that the new image downloaded properly.

   The status of the update is displayed in the TFTP Update Status pane.

### CLI Command

To download new application software from a TFTP server to an APP memory location by using the CLI, use the following command:

**(configure)# copy tftp flash {app1 | app2} {cardapp1 | cardapp2} <*image_opt_path*> <*ip-addr*>**

For more information on this command, see Chapter 27, "System," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches.*

# Setting the Startup Image

After you download the new software, you must set the switch to load the new software at startup. You can use either the Web Agent or CLI to perform this task.

### Web Agent Procedure

To set the switch to load the new software at startup:

1. In the navigation pane, expand the **System** > **Memory** folders.
2. Select **FEPROM**.

The **FEPROM Contents** Web page is displayed in the content pane (Figure A-183).

3. In the **Power Up/Reset Image** field, select the APP location to which you downloaded the new application software.

4. Select **APPLY**.

### CLI Command

To set the switch to load the new software at startup, use the following CLI command:

**<configure># boot system flash {app1 | app2 | cardapp1 | cardapp2}**

For more information on this command, see Chapter 27, "System," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches.*

# Synchronizing the Active and Standby Supervisor Modules

If the switch has a redundant supervisor module, you must synchronize the active and standby supervisor modules after you upgrade the application software on the active supervisor module. During this synchronization, the new boot code and application software are copied to the standby supervisor module.

For information on how to synchronize the active and standby supervisor modules, see "Synchronizing the Active and Standby CPUs" on page 7-14.

CAUTION

**The Avaya Multiservice Switch must have the same model supervisors in slots 1 and 2 to support redundant supervisor operation. Both Active and Standby CPUs app1 and app2 images must run 5.0 or greater software to support 80-series Supervisor.**

CAUTION

**The Standby supervisor module must use the same boot code as the Active Supervisor module and must be running in the same Fabric mode.**

CAUTION

**When making configuration changes to the switch you must save the changes you made by copying the running**

**configuration file to the startup configuration file. This ensures that the changes persist after the switch is restarted. When your switch is configured with a redundant supervisor, you must also synchronize the supervisor modules in order for both to have the same configuration and reset the standby.**

# Resetting the Active Supervisor

After setting the switch to load the new software at startup, you must reset the switch. You can use either the Web Agent or CLI to perform this task.

If the switch has a redundant supervisor module, resetting the Active supervisor to load the new boot and application code forces the Active supervisor to Standby, and the Standby supervisor to the Active Supervisor mode. See, “Reset the Standby Supervisor”, next to change the Supervisor modes back to their original state.

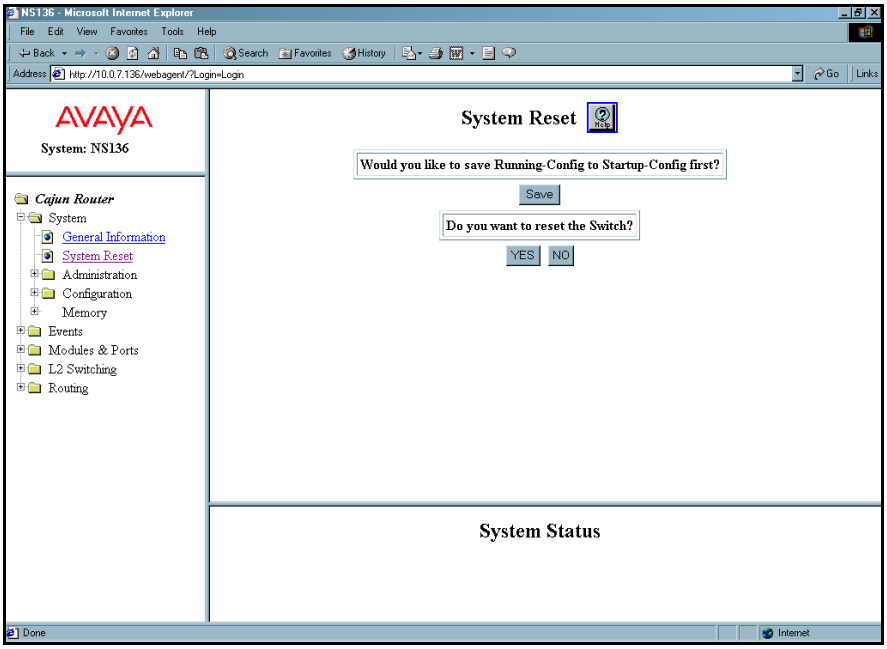
## Web Agent Procedure

To reset the switch after downloading new application software:

1. In the navigation pane, expand the **System** folder.
2. Select **System Reset**.

   The **System Reset** Web page is displayed in the content pane (Figure A-3).

*Figure A-186. System Reset Web Page*




3. Select **Yes** in response to the question, **Do you want to reset the switch?**

   The switch resets and loads the new application software.

### CLI Command

To reset the switch after downloading new application software, use the following CLI command:

**<configure># reset**

For more information on this command, see Chapter 27, “System,” in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches*

# Resetting the Standby Supervisor

In the previous procedure "Resetting the Active Supervisor," the procedure forces the Active Supervisor to the Standby mode and the Standby Supervisor to the Active Supervisor mode. To recover back to the original state, with both supervisors running new code, reset the current Active supervisor module.

### Web Agent Procedure

To reset the Active Supervisor to the Standby Supervisor:

1. In the navigation pane, expand the **System** folder.
2. Select **System Reset**.

   The **System Reset** Web page is displayed in the content pane (Figure A-3).
3. Select **Yes** in response to the question, **Do you want to reset the switch?**

### CLI Command

To reset the switch after downloading new application software, use the following CLI command:

**<configure># reset**

For more information on this command, see Chapter 27, "System," in the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches*

## Verifying the Upgrade

To verify that the old Active supervisor is now the Standby supervisor, the LED display window (marquee) should scroll `Standby` and the code version.

## Upgrading from v4.*x* to v5.*x*

If a redundant supervisor module is running a 4.*x* version of application software, it is not upgraded to v5.*x* if you follow the upgrade procedure that is described earlier in this appendix.

To upgrade the application software from v4.x to v5.*x* on a switch that has a redundant supervisor module, you much upgrade the application software on each supervisor module individually. To perform this task:

1. Back up the current software. For information on how to perform this step, see "Backing Up the Current Software" on page A-2.
2. Back up the previous configuration. For information on how to perform this step, see "Backing Up the Previous Configuration" on page A-3.

3. Download the application software. For information on how to perform this step, see "Downloading Application Software" on page A-5.

   The following error message is displayed after you download v5.*x*. Disregard it.

   ```
   ERROR: Bad file header compressed
   checksum...transfer cancelled.

   ERROR copying file 'm5500r_v5.03.00.bin'
   from TFTP server <10.10.10.10>
   ```

4. Set the startup image. For information on how to perform this step, see "Setting the Startup Image" on page A-6.

5. Synchronize the active and standby supervisor modules. For information on how to perform this step, see "Synchronizing the Active and Standby CPUs" on page 7-14.

6. Reset the active supervisor. The standby supervisor becomes the active supervisor.

   After the initialization process, the switch displays the following message:

   ```
   The Active CPU in slot x has established
   contact with the Standby CPU in slot y
   ```

7. Repeat Step 1 through 6 on the now active supervisor (original standby supervisor).

   The now active supervisor (original standby supervisor) becomes standby again, and the original active supervisor becomes active again.

# Upgrading a Switch with Multiple VLANs Statically Bound to Hunt Group Ports

If the switch has multiple VLANs statically bound to hunt group ports and you want to upgrade from v5.*x*.*x* to v5.3.*x*, you must:

1. Download v5.3 or higher.

2. Reset the switch to load this software.

3. Delete all hunt groups to which you want to statically bind multiple VLANs.

4. Use the CLI command to statically bind the VLANs to every port that you want to assign to a hunt group.

   *** Note:** For the appropriate CLI command to use, refer to the CLI Reference Guide.

5. Assign the ports to hunt groups.

6. Save the running configuration to the startup configuration.

# B Boot Mode

Boot Mode is a special mode for the Avaya P550R/P580/P880/P882 Multiservice switch. Boot mode is used to:

- Recover your password
- Download new operational code

## Accessing BOOT Mode

You can access BOOT mode during Power Up or when both Operational Images in APP1 and APP2 are corrupted.

### Accessing BOOT Mode During Power Up

To access BOOT mode during power up:

1. Power-Off the Switch.
2. Connect a console to the supervisor Module (refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*, "Chapter 3, Configuration").
3. Press and Hold the DISPLAY button on the supervisor module as you Power-on the switch until the boot prompt displays on the console.

### Accessing BOOT Mode with Corrupted Operational Images

The Avaya P550R/P580/P880/P882 Multiservice switch will automatically come up in BOOT mode if both operational images are corrupted.

You will see the following output on your console:

```
Starting the boot system, please wait.
Initializing the event subsystem ... done
Initializing the platform ... done
```

```
Starting up threads ...
    Periodic Task
    Network Interface
    Front Panel Display
    Download
    Command Line Parser

Boot process complete - system is now operational.

Boot Software Revision: V5.3

Press Ctrl-P for previous command, Ctrl-N for next command


download   Download to FEPROM
feprom     Flash EPROM configuration
initLogins Restore default passwords
ip         IP Configuration
manuf      Get/Set MAC address
nvram      Initializes NV RAM-diags run upon reboot
peek       Read from memory
ping       Ping host [tries] [delay]
poke       Write to memory
reset      Reset System

Boot>
```

## Password Recovery

The following command is used to reset the switch to the factory default passwords.

initLogins

### Syntax

```
Boot> initLogins set <0=no change, 1=factory default>
```

### Description

Using a value of zero will retain the current passwords in NVRAM upon resetting the switch. Using a value of one will restore the factory default passwords in NVRAM upon resetting the switch.

## Downloading New Operational Code

To download new operational code in BOOT mode into APP1 or APP2.

*** Note:** The Avaya P550R/P580/P880/P882 Multiservice switch does not have an IP address assigned to the console ethernet port when it comes up in BOOT mode. Therefore, a user must assign an IP address (and default

gateway) to the ethernet console port prior to attempting the TFTP download of a new operational image.

1. Ensure the ethernet console port is connected to the network for a TFTP transfer (refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1*, "Chapter 3, Configuration").

2. Enter the following command to assign an IP address to the ethernet console port:

   ```
   Boot> ip address <ip address> <ip mask>
   ```

3. Enter the following command to assign a default gateway to the ethernet console port (if necessary):

   ```
   Boot> ip default_gateway <ip address>
   ```

4. Enter the following command to download new operational code to APP1 or APP2:

   ```
   Boot> download <app1|app2> <serverIP> <filename>
   ```

5. Enter the following command to set the switch to boot from the appropriate image stored in APP1 or APP2

   ```
   Boot> feprom set <app1|app2>
   ```

6. Enter the following command to reset the switch:

   ```
   Boot> reset
   ```

# C Supported MIB Groups

The following section lists, by protocol, public and private MIBs supported by the Avaya P550R, P580, P880, and P882 Multiservice switches.

## General Private MIBs

The following general private MIBs are supported:

- Avayacjnroot.mib
- Avayagen.mib
- Aveisprod.mib
- cjnRoot.mib
- cjnSwitchRoot.mib
- genlic.mib
- ProminetMIB.txt

## IPX Interface MIBs

### Private IPX Interface MIBs

The following private IPX interface MIBs are supported:

- cjnipxifmgmt.mib
- cjnipx.mib
- cjnipxrip.mib
- cjnipxsap.mib

## IEEE 802.3 MAU Management

RFC 1155 is supported.

## IEEE 802.3 Statistics Group

RFC 1398 is supported.

## Bridge MIB

RFC 1493 is supported.

## SNMPv2

RFC 1907 is supported.

## RMON

RFC 1757 is supported.

## RMON2 MIB

The standard MIB RFC 2021 is supported for Trap Destination Table.

## SMON

The standard MIB RFC 2613 is supported.

The Private MIB cjnportcopyext.mib is supported.

## RIP Version 1.0 and 2.0

### Standard MIB

RFC 1724 is supported.

### Private MIB

The private MIB cjniprip.mib is supported.

## OSPF Version 2.0

### Standard MIB

RFC 1850 is supported.

### Private MIB

The private MIB cjnospf.mib is supported.

## VRRP

### Standard MIB

The current draft of the Virtual Redundancy Router Protocol (VRRP) MIB is supported: draft-ietf-vrrp-mib-04.mib.

### Private MIB

The private MIB cjniplrrp.mib is supported.

## IGMP

### Standard MIB

The current draft of the Internet Group Membership Protocol (IGMP) MIB is supported: draft-ietf-idmr-igmp-mib-07.mib.

### Private MIB

The private MIB cjnigmp.mib is supported.

## IP Interface

The standard MIB RFC 2863 is supported.

The private MIB cjnipifmgmt.mib is supported.

## IP Version 4.0 and Services

### Standard MIB

The following standard MIBs for Internet Protocol version 4.0 and services are supported:

- RFC 1213
- RFC 2011
- RFC 2012
- RFC 2013

### Private MIB

The following private MIBs are supported for Internet Protocol version 4.0 and services:

- cjnipv4.mib
- cjnipv4serv.mib

## IP Forwarding/Route Table

**Standard MIB** RFC 2096 is supported.

**Private MIB** The private MIB l3fwd.mib is supported.

## DVMRP

**Standard MIB** The current draft of the DVMRP MIB is supported: draft-thaler-dvmrp-mib-9.mib.

**Private MIB** The private MIB cjndvmrp.mib is supported.

## AppleTalk

**Standard MIB** RFC 1243 is supported.

**Private MIB** The private MIB cjnatalk.mib is supported.

## Policy Capability MIB for LDAP

The private MIB that defines policy capabilities for the Lightweight Directory Access Protocol (LDAP), cjnpolicycap.mib, is supported.

## Load MIB

The Load MIB (load.mib)defines upload, download and copy of application software and configuration information.

# D FCC Notice

**FCC Notice** — Class A Computing Device:

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference. Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference. Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

**VCCI Notice** — Class A Computing Device:

This equipment is in the Class A category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in commercial and/or industrial areas. Consequently, when used in a residential area or in an adjacent area thereto, radio interference may be caused to radios and TV receivers. Read the instructions for correct handling.

**CE Notice** — Class A Computing Device:

**Warning!**

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

**Achtung!**

Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

**Avertissement!**

Cet appareil est un appareil de Classe A. Dans un environnement résidentiel cet appareil peut provoquer des brouillages radioélectriques. Dans ce cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.

# Index

## Numerics


10/100 port
  auto negotiation speed/duplex advertisement, 5-22
10/100 port parameter
  auto-negotiation mode, 5-22
  category, 5-21
  duplex mode, 5-21
  flow control mode, 5-21
  name, 5-21
  port PACE priority, 5-22
  rate limit burst size, 5-22
  rate limit mode, 5-22
  rate limit rate, 5-22
  speed mode, 5-21
10Base-T crossover patch cables, 2-8
10-port 100BASE-FX, 1-10
12-port 10/100BASE-TX, 1-10
3Com mapping table
  non-VLAN switch port parameters, 5-28
  switch port configuration parameters, 5-29


## A


AARP invalid PDU
  AppleTalk global statistics, 15-26
AARP reply rx
  AppleTalk global statistics, 15-26
AARP reply tx
  AppleTalk global statistics, 15-26
AARP req rx
  AppleTalk global statistics, 15-26
AARP req tx
  AppleTalk global statistics, 15-26
access level
  configuring SNMP communities, 2-21
access list
  AppleTalk NBP filter parameters, 15-17
  AppleTalk zone filter parameters, 15-21
access list name
  IP access list parameters, 9-23, 9-26
access list rules
  IP interface, 9-21
access lists
  IP interface, 9-17
access rule index
  IP access list parameters, 9-23, 9-26
access type
  IP access list parameters, 9-24, 9-26
Accessible Features, 2-16, 2-23
Accessing BOOT Mode, B-1
active alarm table
  viewing, 17-5, 17-6
active alarms
  checking, 17-5
active backpressure, 5-21
add IP interface parameters
  admin. state, 9-8
  ICMP redirect, 9-9
  interface, 9-7
  IP routing, 9-8
  MAC format, 9-8
  mask, 9-8
  multicast protocol, 9-9
  NetBIOS UDP rebroadcast, 9-9
  network address, 9-8
  OSPF, 9-9
  proxy ARP, 9-9
  RIP, 9-9
  VLAN, 9-7
  VRRP, 9-9
adding a user, 2-15, 2-17, 2-19
  password, 2-18
  user logins, 2-17
adding address forward table entries manually, 6-21
Adding Entries to the AFT Manually Using the Web Agent, 6-21
addr owner override
  VRRP configuration parameters, 9-100
address age time
  definition, 6-9
address forwarding table, 6-1
  adding entries manually, 6-21
  capacity, 6-15
address forwarding table parameters
  group, 6-19
  index, 6-19
  MAC address, 6-19
  persistence, 6-20
  port, 6-19
  priority, 6-19
  status, 6-20
  TblInst, 6-19
  valid, 6-19
address forwarding table, persistence parameters
  ageout, 6-22
  permanent, 6-22
address mask
  DVMRP interface statistical parameters, 9-82
address table instance
  delete all learned entries, 6-14

delete invalid learned entries, 6-14
address table instance entry type
learned, 6-13
management, 6-13
multicast, 6-13
self, 6-13
address table instance hash table
auto increment, 6-14
size, 6-14
address table instance parameters
bucket info, 6-14
entry type, 6-13
entry validity, 6-13
hash table, 6-14
total number of entries, 6-13
VLAN association, 6-13
address table sizes
controlling reconfiguration, 6-15
address table, age timer
configuring, 6-9
address table, super age timer
configuring, 6-9
admin
SNMP security level, 2-22
admin state
AppleTalk interface parameters, 15-7
IPX interface, 12-8
admin. state
add IP interface parameters, 9-8
adv. address
IRDP parameters, 9-107
advertisement
OSPF summaries parameters, 11-19
advertisement life time
IRDP parameters, 9-107
advertisement timer
VRRP configuration parameters, 9-99
advertisements received
VRRP statistical parameters, 9-102
advertisements sent
VRRP statistical parameters, 9-102
age
LSA detail, 11-32
OSPF link state database parameter, 11-31
age interval
Layer 3 cache configuration, 18-3
age timer
buffer management table parameters, 20-5
aged entries
forwarding cache (FE) parameters, 18-11
ageout
address forwarding table, persistence parameters, 6-22
persistence entry, 6-20
aggregating bandwidth, 4-28
aging
Layer 3 cache configuration, 18-3
aging interval multiplier
IPX SAP interface parameters, 14-2
alarms
log size, setting, 17-16
system events, activating, 17-16
alarms, event log
definition, 17-17
alarms, shutdown log
definition, 17-17
all module ports configuration, 5-23
allow learning
non-VLAN switch port parameters, 5-27
switch port configuration parameters, 5-29
always be group membership querier
IGMP interface parameters, 9-56
APP1
CPU redundancy configuration, 7-18
APP2
CPU redundancy configuration, 7-18
AppleTalk
creating an NBP filter, 15-16
ethernet versions supported, 15-2
event class parameters, 17-18
AppleTalk ARP cache table
viewing, 15-31, 15-32
AppleTalk ARP cache table statistics
interface, 15-32
MAC address, 15-32
network range, 15-32
node, 15-32
TTL, 15-32
type, 15-32
AppleTalk global routing
enabling, 15-4
AppleTalk global statistics
AARP invalid PDU, 15-26
AARP reply rx, 15-26
AARP reply tx, 15-26
AARP req rx, 15-26
AARP req tx, 15-26
Bcast error, 15-26
checksum error, 15-26
config addr error, 15-26
config zone error, 15-26
DDP forward counter, 15-26
DDP input counter, 15-26
DDP local counter, 15-26
DDP output counter, 15-25
DDP output long, 15-26
DDP output short, 15-25

echo reply rx, 15-25
echo req rx, 15-25
echo req tx, 15-25
no client, 15-26
no route, 15-26
RTMP RDR Rx, 15-26
RTMP RDR Tx, 15-26
RTMP Rq Rx, 15-26
RTMP Rq Tx, 15-26
RTMP Rsp Rx, 15-26
RTMP Rsp Tx, 15-26
Short PDU in error, 15-26
too long, 15-26
too short, 15-26
TTL expired, 15-26
viewing, 15-24, 15-27
Zip Ext Reply Rx, 15-26
Zip Ext Reply Tx, 15-27
Zip GNI Rq Rx, 15-27
Zip GNI Rq Tx, 15-27
Zip GNI Rsp Rx, 15-27
Zip GNI Rsp Tx, 15-27
Zip Query Rx, 15-26
Zip Query Tx, 15-26
Zip Reply Rx, 15-26
Zip Reply Tx, 15-26
AppleTalk interface
deleting, 15-10, 15-11
AppleTalk interface parameters
admin starte, 15-7
encapsulation type, 15-6
interface, 15-6
metric, 15-6
network number, 15-7
network range end, 15-7
network range start, 15-7
node, 15-7
VLAN, 15-6
zone, 15-7
AppleTalk interface statistics
interface, 15-28
network number, 15-28
network range, 15-28
node, 15-28
seed, 15-28
state, 15-28
AppleTalk interface, creating, 15-5, 15-8
AppleTalk interface, editing, 15-8, 15-10
AppleTalk NBP filter
editing, 15-18
AppleTalk NBP filter parameters
access list, 15-17
interface, 15-17
name, 15-17
type, 15-17
AppleTalk NBP table
viewing, 15-34, 15-35
AppleTalk NBP table parameters
index, 15-35
interface, 15-35
name, 15-35
type, 15-35
zone, 15-35
AppleTalk overview, 15-1
AppleTalk protocols
supported, 15-2
AppleTalk route table
viewing, 15-29
AppleTalk route table statistics
current number of routes, 15-31
interface, 15-30
metric, 15-29
network range, 15-29
next hop, 15-29
owner, 15-29
peak number of routes, 15-31
state, 15-29
zones, 15-30
AppleTalk route table statistics, viewing, 15-30
AppleTalk routing overview, 15-1
AppleTalk routing, configuring, 15-3
AppleTalk static route
creating, 15-11
deleting, 15-15
editing, 15-13, 15-15
network number, 15-12
network range end, 15-12
network range start, 15-12
node, 15-13
type, 15-13
zone, 15-13
AppleTalk statistics
viewing, 15-24
AppleTalk zone filter
creating, 15-20
editing, 15-22
AppleTalk zone filter parameters
access list, 15-21
interface, 15-21
name, 15-21
type, 15-21
AppleTalk zone table
viewing, 15-33
AppleTalk zone table statistics
current number of zones, 15-34
index, 15-33
name, 15-33

network range, 15-33
peak number of zones, 15-34
AppleTalk zone table statistics, viewing, 15-33, 15-34
application
multicast session client port parameters, 16-14
multicast session parameters, 16-12
router port display parameters, 16-9
area
LSA detail, 11-32
OSPF interface parameters, 11-11
OSPF summaries parameters, 11-19
OSPF virtual link parameters, 11-15
area ID
OSPF area parameters, 11-6
OSPF link parameters, 11-24
OSPF link state database parameter, 11-30
OSPF link state database search parameters, 11-29
OSPF statistical parameters, 11-23
area type
OSPF area parameters, 11-6
ARP cache
searching, 9-71
ARP cache entries, 9-13
ARP cache search parameters
IP address, 9-72
VLAN, 9-72
AS border route
OSPF global configuration parameters, 11-4
AS border Rtrs
OSPF statistical parameters, 11-23
ASBR, 11-4
ATM
overview, 1-7
attached router ID 1 & 2
LSA detail, 11-32
auth key
RIP interface parameters, 10-6
VRRP configuration parameters, 9-99
auth type
RIP interface parameters, 10-6
authentication
OSPF interface parameters, 11-11
OSPF virtual link parameters, 11-16
authentication failure
event class parameters, 17-17
authentication key
OSPF virtual link parameters, 11-16
Authorization Type, 9-99
auto increment
address table instance hash table parameter, 6-14
auto increment HT size
VLAN configuration parameters, 4-10
auto negotiation speed/duplex advertisement
10/100 port, 5-22
auto-creation of virtual links
OSPF global configuration parameters, 11-4
automatic client pruning
automatic client pruning, 16-7
automatic router pruning
automatic router pruning, 16-7
automatic session pruning
automatic session pruning, 16-7
automatic VLAN creation, 4-5, 4-7, 5-27
Cisco Catalyst 5000 parameters, 5-30
switch port configuration parameters, 5-28
auto-negotiation
Fast Ethernet module, 5-19
auto-negotiation mode
10/100 port parameter, 5-22

## *B*

bad advertisements received
VRRP statistical parameters, 9-102
bad packets received
IPX SAP interface statistical parameters, 13-9, 14-14
RIP statistical parameters, 10-11, 10-13
bad routes received
RIP statistical parameters, 10-11, 10-13
baud rate
console serial port settings, 2-34
Bcast error
AppleTalk global statistics, 15-26
BDR address
OSPF link parameters, 11-24
BDR choice
OSPF neighbors parameters, 11-27
bind to all
Virtual LAN binding options, 5-31
bind to received
Virtual LAN binding options, 5-31
Binding a Port to more than one VLAN with the CLI, 4-6
binding options
Virtual LANs, 5-31
binding type
VLAN switch port table parameters, 4-12
blocking state (spanning tree bridge port), 4-22
BOOTP relay agent, 9-46, 9-47
BOOTP/DHCP in discards
IP routing global statistics, 9-68
BOOTP/DHCP in hops exceeded
IP routing global statistics, 9-68
BOOTP/DHCP in requests
IP routing global statistics, 9-68
BOOTP/DHCP in responses
IP routing global statistics, 9-68
BOOTP/DHCP out requests
IP routing global statistics, 9-68

BOOTP/DHCP out responses
IP routing global statistics, 9-68
BOOTP/DHCP relay agent
IP global configuration parameters, 9-13
border Rtrs
OSPF statistical parameters, 11-23
bridge forward delay
spanning tree bridge level parameters, 4-19
bridge hello time
spanning tree bridge level parameters, 4-19
bridge max age
spanning tree bridge level parameters, 4-19
bridge port
spanning tree bridge port parameters, 4-21
bridge port parameters
bridge port, 4-21
designated bridge, 4-22
designated cost, 4-22
designated port, 4-22
designated root, 4-22
forward transitions, 4-22
name, 4-21
port, 4-21
state, 4-22
bridge ports
configuring, 4-20
bridge status
event class parameters, 17-18
broadcast packets
Ethernet interface statistical parameters, 19-4
bucket info
address table instance parameters, 6-14
buffer and queue management,overview, 1-21
buffer detailed configuration parameters
memory, 20-5
buffer management parameters
fabric port buffers, 20-4
physical port buffers, 20-4
buffer management table parameters
age timer, 20-5
congestion drops, 20-6
high and normal overflow drops, 20-6
high and normal stale drops, 20-6
high priority allocation, 20-6
high priority service ratio, 20-6
priority threshold, 20-6
buffers
managing, 20-2, 20-7
bytes
Ethernet interface statistical parameters, 19-4

## *C*

CajunDocs CD, -xxii
Cajun-Service-Type required
RADIUS configuration parameters, 2-31
category
10/100 port parameter, 5-21
gigabit port parameters, 5-15
CGMP packet reception statistics
CGMP snooping parameters, 16-37
CGMP snooper, configuring/viewing
configuring CGMP snooper, 16-36, 16-37, 16-38
CGMP snooping parameters
CGMP packet reception statistics, 16-37
enable state, 16-37
intelligent multicast session statistics, 16-37
checking active alarms, 17-5
checksum
IPX datagram fields, 12-2
LSA detail, 11-32
OSPF link state database parameter, 11-31
checksum error
AppleTalk global statistics, 15-26
Cisco Catalyst 5000 parameters
port VLAN, 5-30
Cisco Catalyst 5000, parameters
automatic VLAN creation, 5-30
trunk mode, 5-30
VLAN binding, 5-30
VTP snooping, 5-30
CLI
regaining access, 2-40
CLI configuration
supervisor module, 2-4
client port
multicast session parameters, 16-12
client pruning timer
client pruning timer, 16-7
clients per VLAN, displaying, 16-35
collisions, 19-7
communities
configuring SNMP, 2-20, 2-23
SNMP, 2-20
Community String, 2-21
comparison value
Layer 3 route cache search parameters, 18-8
config addr error
AppleTalk global statistics, 15-26
config zone error
AppleTalk global statistics, 15-26
configuration
event class parameters, 17-17
invalid copies, 2-52
saving, A-3
configuration file management
copy destination, 2-51

copy source, 2-50
destination filename, 2-51
save running configuration to startup configuration, 2-50
source filename, 2-51
TFTP server IP address, 2-51
configuration files, 2-46
configuration revision number
VTP snooping parameters, 4-48
configure, 16-9, 16-10
configure ports
gigabit module, 5-12, 5-16, 5-23
configure source
port mirroring information parameters, 19-9
configure static router ports
static router ports, 16-9, 16-10
configuring
switch port, 5-24
configuring a DNS client, 8-1
configuring a Fast Ethernet module, 5-17
configuring a redundant CPU, 7-11
configuring a redundant element, 7-10
configuring all VLAN ports, 4-11
configuring an IPX router, 12-4, 12-5
configuring AppleTalk routing, 15-3
configuring event logs, protocol, 17-7, 17-12
Configuring Event Notification, 17-19
configuring event notification, 17-19
Configuring Fast Start Mode, 5-33
configuring fast start mode, 5-33, 5-34
Configuring Fast Start Mode Using the Web Agent, 5-33, 5-34
configuring flow control mode
gigabit module, 5-14, 5-19
configuring hunt groups, 4-36
configuring IGMP, 9-51
configuring IGMP interfaces, 9-55
Configuring IGMP Snooping, 16-22, 16-27
configuring IGMP snooping, 16-22, 16-23
configuring IP global routing, 9-11
configuring IP interface access lists, 9-17
configuring IP interfaces, 9-6
Configuring IPX Routing Globally, 12-4
configuring IPX SAP interfaces, 14-1
Configuring LDAP Setting from the Web Agent, 9-110, 9-112
configuring multiple interfaces on a VLAN, 9-14
configuring physical port parameters
gigabit ports, 5-15
configuring RADIUS client, 2-29, 2-31
configuring RIP global configuration, 10-1
configuring RMON mirror port, 19-8
configuring service port
gigabit module, 5-14, 5-18
Configuring Spanning Tree Bridge Ports Using the CLI, 4-24
configuring the address table age timer, 6-9
configuring the address table super age timer, 6-9
Configuring the Age Timer and Super Age Timer Using the Web Agent, 6-10
Configuring the IP Interface for the PPP Console, 9-116, 9-118
configuring the LGMP server, 16-26, 16-27, 16-28, 16-30
configuring the PPP console static route, 9-115
configuring the serial port console
PPP console, 2-36
configuring the supervisor module
using the CLI, 2-4
configuring the temperature system, 3-12, 3-13
configuring thresholds, 17-2
configuring user port
gigabit module, 5-14, 5-18
Configuring VLAN Parameters, 4-11
configuring VRRP, 9-93
congestion drops
buffer management table parameters, 20-6
connecting a modem, 2-35
overview, 2-35
console serial port
changing, 2-32
console serial port settings, changing
baud rate, 2-34
data bits, 2-34
flow control, 2-34
parity, 2-34
stop bits, 2-34
consumer signal
LDAP statistics, 9-114
contacting Lucent, -xv
contacting Lucent technical support, -xv
controlling address table size reconfiguration, 6-15
conventions, -xvi
cooling system status
displaying, 3-15
copy destination
configuration file management, 2-51
copy source
configuration file management, 2-50
copying
configuration
invalid combinations, 2-52
from the switch or server to a configuration file, 2-49
running configuration to startup configuration, 2-48, 2-49, 2-53
startup configuration to running configuration, 2-49
to a TFTP server, 2-49
to the switch, 2-49

copying files, 2-51
copying from/to a TFTP server, 2-51
copying source files, 2-49
cost
IP static route parameters, 9-44
OSPF interface parameters, 11-11
CPU redundancy configuration
APP1, 7-18
APP2, 7-18
power-up/reset image, 7-18
startup config, 7-18
status, 7-18
CRC alignment errors
Ethernet interface statistical parameters, 19-5
create a Custom Access Typ, 2-14
Create Custom Access Type, 2-14
Creating 3Com Mapping Tables Using the Web Agent, 4-13
creating a BOOTP/DHCP server entry, 9-46, 9-47
creating a multinet interface, 9-15
creating a static client port, 16-18, 16-19
creating a VRRP router, 9-96
creating access rules for filtering traffic between subnets, 9-30
creating an AppleTalk interface, 15-5, 15-8
creating an AppleTalk static route, 15-11
creating an AppleTalk zone filter, 15-20
creating an IP interface, 9-4, 9-9
creating an IPX interface, 12-5, 12-9
creating an NBP filter
AppleTalk, 15-16
creating an VRRP virtual router, 9-96, 9-100
Creating Hunt Groups, 4-36
Creating Hunt Groups Using the CLI, 4-41
creating IP interface access list rules, 9-21
creating IPX RIP filters, 13-3, 13-7, 13-8
creating IPX SAP filters, 14-3, 14-4
Creating IPX SAP Name Filters Using the Web Agent, 14-4
creating IPX SAP network filters, 14-8, 14-12
creating IPX static routes, 12-10, 12-12
Creating IPX Static Routes Using the CLI, 12-12
creating IPX static services, 12-14, 12-16
Creating IPX Static Services Using the CLI, 12-16
creating OSPF summaries, 11-18, 11-19, 11-20
Creating OSPF Summaries Using the Web Agent, 11-18
creating OSPF virtual links, 11-14, 11-16
Creating Standard Access Rules, 9-21
creating static ARP entries
IP static route, 9-45
Creating Static Client Ports, 16-18
creating static IP routes, 9-43
Creating Trusted RIP Neighbors Using the Web Agent, 10-7
Crossbar, 1-4, 1-6
crossbar features supported, 1-5, 1-7
current entries
forwarding cache (FE) parameters, 18-11
current number of routes
AppleTalk route table statistics, 15-31
DVMRP routing statistical parameters, 9-85
IP routing table statistical parameters, 9-71
current number of zones
AppleTalk zone table statistics, 15-34
current power available
power system statistical parameters, 3-14
Custom Access Types, 2-13, 2-15, 2-16

# *D*

data bits
console serial port settings, 2-34
day
summer time hours configuration, 3-8
DD number
OSPF neighbors parameters, 11-26
DDP forward counter
AppleTalk global statistics, 15-26
DDP input counter
AppleTalk global statistics, 15-26
DDP local counter
AppleTalk global statistics, 15-26
DDP output counter
AppleTalk global statistics, 15-25
DDP output long
AppleTalk global statistics, 15-26
DDP output short
AppleTalk global statistics, 15-25
dead interval
OSPF interface parameters, 11-11
OSPF virtual link parameters, 11-16
debug
protocol event log settings, 17-12
default metric
RIP interface parameters, 10-5
default password, 2-6
default route
RIP interface parameters, 10-5
delete a custom access type, 2-16
Delete Custom Access Type, 2-16
deleting an AppleTalk interface, 15-10, 15-11
Deleting an AppleTalk Interface Using the CLI, 15-11
Deleting an AppleTalk Static Route Using the Web Agent, 15-15
deleting an OSPF area, 11-7, 11-8
deleting AppleTalk static routes, 15-15
deleting OSPF virtual links, 11-16

Deleting Static Client Ports, 16-19
deleting static client ports, 16-19, 16-20
Deleting Static Client Ports Using the CLI, 16-20
description
event and shutdown log entries, 17-14
designated bridge
spanning tree bridge port parameters, 4-22
designated cost
spanning tree bridge port parameters, 4-22
designated forwarder
DVMRP route table parameters, 9-86
designated forwarder(s) table parameters
forwarder cost to source network, 9-88
forwarder network address, 9-88
forwarding interface, 9-88
designated port
spanning tree bridge port parameters, 4-22
designated root
spanning tree bridge port parameters, 4-22
destination address
Layer 3 route cache search parameters, 18-7
destination filename
configuration file management, 2-51
destination group address
DVMRP downstream link parameters, 9-91, 9-92
DVMRP multicast forwarding cache parameters, 9-90
DVMRP upstream source parameters, 9-92
IGMP local multicast forwarding cache parameters, 9-79
upstream prune information, 9-91
destination network
IPX datagram fields, 12-3
destination node
IPX datagram fields, 12-3
destination port
Layer 3 route cache search parameters, 18-8
destination port number
DVMRP upstream source parameters, 9-92
destination socket
IPX datagram fields, 12-3
destination subnet
IP access list parameters, 9-26
detail link
OSPF link state database parameter, 11-30
diagnostics
for switch hardware, 7-4
direction
IPX RIP filter parameters, 13-5
IPX SAP filter parameters, 14-6
IPX SAP network filter parameters, 14-10
disabled (spanning tree bridge port), 4-22
disabling, 4-24
Disabling Spanning Tree Mode for the Port Using the Web Agent, 4-25
Disabling Spanning Tree Mode on a Port Using the CLI, 4-28
displaying
intelligent multicasting, 16-8
IPX routing global statistics, 12-18, 12-19
displaying DVMRP global statistics, 9-79
displaying DVMRP multicast forwarding cache, 9-89
displaying DVMRP routing table statistics, 9-84
displaying frame forwarding cache statistics, 18-4
Displaying Global IP Routing Statistics, 9-62
displaying global IP routing statistics, 9-62, 9-71
displaying IGMP global statistics, 9-73
displaying IGMP local multicast forwarding cache, 9-78
displaying IPX RIP interface statistics, 7-1
displaying Layer 3 forwarding cache, 18-9
displaying multicast forwarding cache, 9-89
Displaying OSPF Links Using the Web Agent, 11-24
displaying OSPF neighbors, 11-25
Displaying OSPF Neighbors Using the Web Agent, 11-25
displaying OSPF statistics, 11-21
displaying router ports, 16-8
displaying the cooling system status, 3-15
displaying the DVMRP designated forwarder table, 9-87
displaying the DVMRP routing table, 9-85
Displaying the Forwarding Cache, 18-9
displaying the IGMP multicast group table, 9-77
displaying the power system statistics, 3-13
DNS client
configuring, 8-1
document conventions, -xvi
documentation
feedback, -xxiii
online, -xviii
documentation feedback, -xxiii
domain name
VTP snooping parameters, 4-48
down state (spanning tree bridge port), 4-22
downloaded image
viewing, A-6
downloading image from TFTP server to an APP location, A-5
downstream dependent router
DVMRP route table parameters, 9-86
downstream interface
DVMRP multicast forwarding cache parameters, 9-91
downstream interfaces
IGMP local multicast forwarding cache parameters, 9-79
DR address
OSPF link parameters, 11-24
DR choice

OSPF neighbors parameters, 11-27
DR priority
OSPF interface parameters, 11-11
OSPF neighbors parameters, 11-27
DR router ID
OSPF link parameters, 11-24
DUAL-LAYER SPANNING TREE, 1-19
duplex mode
10/100 port parameter, 5-21
duplicate add attempts
forwarding cache (FE) parameters, 18-11
DVMRP
configuring, 9-57
displaying global statistics, 9-79
modifying information, 9-59
DVMRP designated forwarder table
displaying, 9-87
DVMRP downstream dependent router
DVMRP supported major/minor version, 9-89
found on interface, 9-88
router is SNMP manageable, 9-89
router network address, 9-88
router received probe from this router, 9-89
router supports generation ID function, 9-89
router supports prune function, 9-89
DVMRP downstream interface
DVMRP downstream link parameters, 9-92
DVMRP downstream link parameters
destination group address, 9-91, 9-92
DVMRP downstream interface, 9-92
interface is pruned, 9-92
interface type, 9-92
prune expiration, 9-92
source subnetwork, 9-92
DVMRP downstream routers
viewing, 9-88
DVMRP global statistical parameters
graft acknowledgments received, 9-80
graft acknowledgments transmitted, 9-81
graft messages received, 9-80
graft messages transmitted, 9-81
probe message received, 9-80
probe messages transmitted, 9-80
prune messages received, 9-80
prune messages transmitted, 9-81
report messages received, 9-80
report messages transmitted, 9-80
unknown messages codes encountered, 9-80
DVMRP interface
modifying, 9-59
DVMRP interface parameters
interface, 9-60
interface metric, 9-60
interface scope, 9-61
interface type, 9-60
IP address, 9-60
IP address mask, 9-60
tunnel endpoint address, 9-60
DVMRP interface statistical parameters
address mask, 9-82
IGMP querier interface, 9-82
interface, 9-82
invalid routes received, 9-82
metric, 9-82
neighbor DVMRP routers, 9-82
network address, 9-82
next probe message in sec, 9-82
state, 9-82
type, 9-82
unrecognized packets received, 9-82
DVMRP interface statistics
examining, 9-81
DVMRP multicast forwarding cache
displaying, 9-89
DVMRP multicast forwarding cache parameters
destination group address, 9-90
downstream interface, 9-91
invalid flows from upstream, 9-90
next pruned downstream interface to timeout, 9-91
packets forwarded through cache entry, 9-90
source address mask, 9-90
source subnetwork, 9-90
upstream interface, 9-90
upstream interface is pruned, 9-91
upstream neighbor router address, 9-90
upstream sources, 9-91
DVMRP neighbor routers
DVMRP supported major/minor version, 9-83
expiration period, 9-83
found on interface, 9-83
neighbor is SNMP manageable, 9-84
neighbor network address, 9-83
neighbor received probe from this router, 9-84
neighbor supports generation ID function, 9-84
neighbor supports MTRACE requests, 9-84
neighbor supports prune function, 9-84
viewing, 9-83
DVMRP parameters
maximum number of routes, 9-59
DVMRP route table parameters
designated forwarder, 9-86
downstream dependent router, 9-86
expiration period in sec, 9-86
reporting router, 9-86
reporting router interface, 9-86
route metric, 9-86
source network, 9-86

source network mask, 9-86
upstream router, 9-86
DVMRP routing statistical parameters
current number of routes, 9-85
number of trigger routes, 9-85
number of valid routes, 9-85
DVMRP routing table
displaying, 9-85
DVMRP routing table statistics
displaying, 9-84
DVMRP supported major/minor version
DVMRP downstream dependent router, 9-89
DVMRP neighbor routers, 9-83
DVMRP upstream interface
upstream prune information, 9-91
DVMRP upstream routers
found on interface, 9-87
router cost to source network, 9-87
router network address, 9-87
viewing, 9-87
DVMRP upstream source parameters
destination group address, 9-92
destination port number, 9-92
flow source address, 9-92
flow upstream interface, 9-92
payload protocol type, 9-92
source port number, 9-92
DVMRP upstream sources, 9-92

## *E*

echo reply rx
AppleTalk global statistics, 15-25
echo req rx
AppleTalk global statistics, 15-25
echo req tx
AppleTalk global statistics, 15-25
editing an AppleTalk static route, 15-13, 15-15
editing an AppleTalk zone filter, 15-22
editing an NBP filter, 15-18
editing AppleTalk interfaces, 15-8, 15-10
editing general system information, 3-2
egress rules
VLAN, 4-7
enable
spanning tree bridge port information parameters, 4-23
enable state
CGMP snooping parameters, 16-37
enable state, 16-7
IGMP snooping, 16-21
LGMP client configuration parameters, 16-32
LGMP server configuration parameters, 16-25
RADIUS configuration parameters, 2-30
enabling
enabling IRDP, 9-106
enabling AppleTalk global routing, 15-4
enabling gigabit ports, 5-13, 5-17
enabling SNTP, 3-3, 3-4
Enabling the LGMP Server, 16-26
enabling the rate limit mode
Fast Ethernet module, 5-19
enabling VRRP, 9-93
encapsulation type
AppleTalk interface parameters, 15-6
end
one-time summer time hours configuration, 3-9
summer time hours configuration, 3-7
end network
IPX RIP filter parameters, 13-4
entries removed due to route changes
forwarding cache (FE) parameters, 18-11
entries removed due to route deletes
forwarding cache (FE) parameters, 18-11
entry expiration period in sec
IGMP group membership table parameters, 9-78
entry type
address table instance parameters, 6-13
entry validity
address table instance parameters, 6-13
E-option
OSPF neighbors parameters, 11-27
error
protocol event log settings, 17-11
Ethernet interface statistical parameters
broadcast packets, 19-4
bytes, 19-4
CRC alignment errors, 19-5
fragments, 19-6
interval start, 19-4
jabbers, 19-7
multicast packets, 19-5
oversize packets, 19-6
packets, 19-4
sample, 19-4
undersize packets, 19-6
utilization, 19-4
Ethernet interface statistics
configuring, 19-3
Ethernet statistics, RMON
viewing, 19-1, 19-7
event and shutdown log entries
description, 17-14
event ID, 17-14
log ID, 17-14
severity, 17-14
time stamp, 17-14

type, 17-14
event and shutdown logs
viewing, 17-12, 17-15
event class parameters
AppleTalk, 17-18
authentication failure, 17-17
bridge status, 17-18
configuration, 17-17
fan status, 17-17
LDAP, 17-18
OSPF, 17-18
resource, 17-17
RIP, 17-18
service port status, 17-17
start, 17-17
switch fabric, 17-18
system, 17-17
temperature status, 17-17
user port status, 17-17
event classes, 17-17
event configuration
accessing, 17-16, 17-19
event ID
event and shutdown log entries, 17-14
event log
definition, 17-17
event log (switch event)
definition, 17-6
event log wraps
event statistics, 17-16
event notification
configuring, 17-19
event statistics
event log wraps, 17-16
events dropped due to event system queue full, 17-16
events dropped due to overload of event system, 17-16
viewing, 17-15, 17-16, 17-18, 17-19
events dropped due to event system queue full
event statistics, 17-16
events dropped due to overload of event system
event statistics, 17-16
examining DVMRP interface statistics, 9-81
examining IP routing table statistics, 9-70
example of routing with Layer 2/3, 1-30
expiration period
DVMRP neighbor routers, 9-83
expiration period in sec
DVMRP route table parameters, 9-86
Extensive Fault Tolerance, 1-21
external LSA count
OSPF statistical parameters, 11-22

## *F*

fabric port buffers
buffer management parameters, 20-4
failed add attempts
forwarding cache (FE) parameters, 18-11
failed element, 7-5
fan status
event class parameters, 17-17
Fast Ethernet module
auto-negotiation mode, enabling, 5-19
configuring, 5-17
rate limit mode, enabling, 5-19
Fast Ethernet module, configuring
pace priority mode, 5-20
rate limit rate, 5-20
Fast Ethernet Modules, 1-10
fast start
switch port configuration parameters, 5-29
fast start mode
configuring, 5-33, 5-34
fault
protocol event log settings, 17-11
files
copying, 2-51
startup.txt, 2-46
filter/suppress
IPX RIP filter parameters, 13-5
IPX SAP filter parameters, 14-6
IPX SAP network filter parameters, 14-10
filtering
index, 6-19
MAC address, 6-19
persistence, 6-20
port, 6-19
priority, 6-19
filtering on the MAC address, 6-16
filtering on the VLAN, 6-16
filtering traffic between subnets, 9-30
FIRE fabric port
frame forwarding statistical parameters, 18-5
flooding., 4-1
flow control
console serial port settings, 2-34
flow control mode
10/100 port parameter, 5-21
gigabit port parameters, 5-15
flow source address
DVMRP upstream source parameters, 9-92
flow upstream interface
DVMRP upstream source parameters, 9-92
forward delay
spanning tree bridge level parameters, 4-19

forward transitions
spanning tree bridge port parameters, 4-22
forwarder cost to source network
designated forwarder(s) table parameters, 9-88
forwarder network address
designated forwarder(s) table parameters, 9-88
forwarding cache
configuring, 18-1, 18-3
displaying, 18-9
forwarding cache (FE) parameters
aged entries, 18-11
current entries, 18-11
duplicate add attempts, 18-11
entries removed due to route changes, 18-11
entries removed due to route deletes, 18-11
failed add attempts, 18-11
lookup hits, 18-11
lookup levels, 18-11
lookup misses, 18-11
memory use in bytes, 18-11
mode, 18-11
PRE, 18-11
total entries, 18-11
type, 18-11
forwarding cache statistics
monitoring, 18-4
forwarding interface
designated forwarder(s) table parameters, 9-88
forwarding rules
VLAN, 4-5
forwarding state (spanning tree bridge port), 4-22
found on interface
DVMRP downstream dependent router, 9-88
DVMRP neighbor routers, 9-83
DVMRP upstream routers, 9-87
fragments
Ethernet interface statistical parameters, 19-6
Frame Classification, 1-15
frame format
VLAN switch port table parameters, 4-12
frame forwarding cache
displaying statistics, 18-4
frame forwarding statistical parameters
FIRE fabric port, 18-5
L2 frame count, 18-6
L3 drop frames, 18-6
L3 frame cache hits, 18-5
L3 slow path frames, 18-5
L3 total (T2), 18-5
percent cache hits, 18-5
percent drops, 18-6
percent slow path, 18-5
RX frame count (T2), 18-6
Frame Tags, 5-26
frame tags
switch port configuration parameters, 5-28
frame type
IPX interface, 12-8
front panel LEDs
interpreting, 17-1
front panel LEDs (10/100 module)
port, 17-2

## *G*

general system information, setting
device contact, 3-2
device location, 3-2
switch name, 3-1
get nearest server reply
IPX SAP interface parameters, 14-3
get nearest server reply delay
IPX SAP interface parameters, 14-3
Gigabit Ethernet modules (L2/L3), 1-11
gigabit module
configure ports, 5-12, 5-16, 5-23
gigabit module, configuring
flow control mode, 5-14, 5-19
port name, 5-13, 5-17
ports, 5-13, 5-17
service port, 5-14, 5-18
user port, 5-14, 5-18
gigabit port name
configuring, 5-13, 5-17
gigabit port parameters
category, 5-15
flow control mode, 5-15
port name, 5-15
port PACE priority, 5-16
gigabit ports
configuring physical port parameters, 5-15
enabling, 5-13, 5-17
Gigabit-Speed Modules, 1-11
global configuration, 16-5, 16-8, 16-9
intelligent multicast, 16-5, 16-8, 16-9
GLOBAL DISABLE, 1-20
global RIP
RIP global configuration parameters, 10-2
Globally Enabling VRRP Using the WEeb Agent, 9-93
GNS requests received
IPX SAP interface statistical parameters, 14-14
GNS responses sent
IPX SAP interface statistical parameters, 14-14
graft acknowledgments received
DVMRP global statistical parameters, 9-80
graft acknowledgments transmitted
DVMRP global statistical parameters, 9-81
graft messages received

DVMRP global statistical parameters, 9-80
graft messages transmitted
DVMRP global statistical parameters, 9-81
group
address forwarding table parameters, 6-19
RADIUS configuration parameters, 2-31
group address
IGMP group membership table parameters, 9-77
group created on
IGMP group membership table parameters, 9-78
group join requests received
IGMP interface statistical parameters, 9-76
group leave requests received
IGMP interface statistical parameters, 9-76
group member interface
IGMP group membership table parameters, 9-77
group membership queries received
IGMP global statistic parameters, 9-74
group membership queries transmitted, IGMP global statistic parameters, 9-74
group membership reports received
IGMP global statistic parameters, 9-74
group multicast protocol
IGMP group membership table parameters, 9-78
group reporter address
IGMP group membership table parameters, 9-78
group reports received
IGMP interface statistical parameters, 9-76

## *H*

hardware requirements for routing, 9-2, 12-3
hardware-based routing and bridging, 1-10
hash mode
Layer 3 cache configuration, 18-3
hash table
address table instance parameters, 6-14
hello interval
OSPF interface parameters, 11-11
OSPF virtual link parameters, 11-15
hello time
spanning tree bridge level parameters, 4-19
Help, Online, -xix
high and normal overflow drops
buffer management table parameters, 20-6
high and normal stale drops
buffer management table parameters, 20-6
high priority allocation
buffer management table parameters, 20-6
high priority service ratio
buffer management table parameters, 20-6
high-preference static routes
IP global configuration parameters, 9-14
high-priority traffic, 20-1
hops
IPX RIP filter parameters, 13-5
IPX route table parameter, 12-22
IPX SAP filter parameters, 14-6
IPX SAP network filter parameters, 14-10
IPX service table parameter, 12-25
IPX static route, 12-11
IPX static service parameter, 12-15
hour
summer time hours configuration, 3-8
hunt group
considerations, 4-35
non-VLAN switch port parameters, 5-27
switch port configuration parameters, 5-29
switch port parameter, 5-37
hunt group members
viewing details, 4-42
hunt groups, 1-16
aggregate bandwidth, 4-28
before configuring, 4-28
configuring, 4-36

## *I*

ICMP in address mask reply
IP routing global statistics, 9-66
ICMP in address mask requests
IP routing global statistics, 9-66
ICMP in destination unreachable
IP routing global statistics, 9-66
ICMP in echo replys
IP routing global statistics, 9-66
ICMP in echo requests
IP routing global statistics, 9-66
ICMP in errors
IP routing global statistics, 9-66
ICMP in messages
IP routing global statistics, 9-66
ICMP in parameter problems
IP routing global statistics, 9-66
ICMP in redirects
IP routing global statistics, 9-66
ICMP in source quenches
IP routing global statistics, 9-66
ICMP in time exceeds
IP routing global statistics, 9-66
ICMP in timestamp replys
IP routing global statistics, 9-66
ICMP in timestamp requests
IP routing global statistics, 9-66
ICMP out address mask reply
IP routing global statistics, 9-67
ICMP out address mask requests

IP routing global statistics, 9-67
ICMP out destination unreachable
IP routing global statistics, 9-66
ICMP out echo reply
IP routing global statistics, 9-67
ICMP out echo requests
IP routing global statistics, 9-67
ICMP out errors
IP routing global statistics, 9-66
ICMP out messages
IP routing global statistics, 9-66
ICMP out parameter problems
IP routing global statistics, 9-67
ICMP out redirects
IP routing global statistics, 9-67
ICMP out source quenches
IP routing global statistics, 9-67
ICMP out time exceeded
IP routing global statistics, 9-66
ICMP out timestamp reply
IP routing global statistics, 9-67
ICMP out timestamp request
IP routing global statistics, 9-67
ICMP redirect
add IP interface parameters, 9-9
IEEE 802.3x full duplex flow control,definition, 1-10
IEEE 802.3X PAUSE, 20-2
IEEE802.1D SPANNING TREE, 1-18
IGMP
configuring, 9-51
Global statistics, 9-73, 9-74, 9-76
overview, 9-51
IGMP global statistic parameters
group membership queries received, 9-74
group membership queries transmitted, 9-74
group membership reports received, 9-74
unknown messages received, 9-74
IGMP global statistics
displaying, 9-73
IGMP group membership table parameters
entry expiration period in sec, 9-78
group address, 9-77
group created on, 9-78
group member interface, 9-77
group multicast protocol, 9-78
group reporter address, 9-78
IGMP interface parameters
always be group membership querier, 9-56
IGMP version, 9-56
interface, 9-55
IP address, 9-55
IP address mask, 9-55
maximum groups, 9-56
neighbor querier timeout interval, 9-56
process leave packets, 9-56
query request interval, 9-56
query response interval, 9-56
robustness variable, 9-56
IGMP interface statistical parameters
group join requests received, 9-76
group leave requests received, 9-76
group reports received, 9-76
IGMP version, 9-75
interface, 9-75
IP address, 9-75
IP address mask, 9-75
neighbor querier timeout in sec, 9-76
next query request in sec, 9-75
number of current groups, 9-76
query messages received, 9-76
query messages transmitted, 9-76
robustness variable, 9-75
state, 9-75
this router is group membership querier, 9-75
unknown messages received, 9-76
IGMP interface statistics
viewing, 9-74, 9-76
IGMP interfaces
configuring, 9-55
IGMP local multicast forwarding cache
displaying, 9-78
IGMP local multicast forwarding cache parameters
destination group address, 9-79
downstream interfaces, 9-79
invalid flows from upstream, 9-79
packets forwarded through cache entry, 9-79
source address mask, 9-79
source subnetwork, 9-79
upstream interface, 9-79
upstream source, 9-79
IGMP multicast group table
displaying, 9-77
IGMP Only Multicast Forwarding, 9-51
IGMP querier interface
DVMRP interface statistical parameters, 9-82
IGMP snooping
configuring, 16-22, 16-23
IGMP snooping parameters
enable state, 16-21
intelligent multicast session statistics, 16-21
new client ports added, 16-21
new router ports added, 16-21
new sessions created, 16-21
router ports removed, 16-21
sessions destroyed, 16-21
IGMP version
IGMP interface parameters, 9-56

IGMP interface statistical parameters, 9-75
in max hops exceeded
IPX global parameters, 12-19
index
address forwarding table parameters, 6-19
AppleTalk NBP table parameters, 15-35
AppleTalk zone table statistics, 15-33
info
protocol event log settings, 17-11
ingress rules
VLAN operation, 4-4
initial hash table size
VLAN configuration parameters, 4-10
intelligent multicast, 16-17, 16-18, 16-26, 16-27, 16-28, 16-30, 16-32, 16-33, 16-35, 16-36, 16-37, 16-38
session search, 16-10, 16-13
intelligent multicast global configuration parameters, 16-7
intelligent multicast session statistics
CGMP snooping parameters, 16-37
IGMP snooping, 16-21
LGMP client configuration parameters, 16-32
LGMP client display per VLAN parameters, 16-35
LGMP server configuration parameters, 16-26
LGMP server display per VLAN parameters, 16-29
intelligent multicasting, 16-5, 16-8, 16-9, 16-10
interface
add IP interface parameters, 9-7
AppleTalk ARP cache table statistics, 15-32
AppleTalk interface parameters, 15-6
AppleTalk interface statistics, 15-28
AppleTalk NBP filter parameters, 15-17
AppleTalk NBP table parameters, 15-35
AppleTalk route table statistics, 15-30
AppleTalk zone filter parameters, 15-21
creating a VRRP virtual router, 9-96, 9-100
DVMRP interface parameters, 9-60
DVMRP interface statistical parameters, 9-82
IGMP interface parameters, 9-55
IGMP interface statistical parameters, 9-75
IP interface parameters, 9-8
IP routing table search parameters, 9-69
IPX interface, 12-8
IPX RIP filter parameters, 13-4
IPX route table parameter, 12-21
IPX routing table search parameters, 12-21
IPX SAP filter parameters, 14-5
IPX SAP interface parameters, 14-2
IPX SAP interface statistical parameters, 13-8, 14-13
IPX SAP network filter parameters, 14-9
IPX service table parameter, 12-25
IPX service table search parameter, 12-24
IPX static route, 12-11
IPX static service parameter, 12-15
IRDP parameters, 9-107
OSPF interface parameters, 11-11
RIP interface parameters, 10-4
RIP statistical parameters, 10-13
VRRP configuration parameters, 9-98
VRRP statistical parameters, 9-101
interface is pruned
DVMRP downstream link parameters, 9-92
upstream prune information, 9-91
interface metric
DVMRP interface parameters, 9-60
interface scope
DVMRP interface parameters, 9-61
interface type
DVMRP downstream link parameters, 9-92
DVMRP interface parameters, 9-60
upstream prune information, 9-91
interfaces
adding to NBP filter, 15-19, 15-20, 15-24
adding to zone filter, 15-23, 15-24
deleting from a zone filter, 15-23, 15-24
deleting from NBP filter, 15-19, 15-20, 15-24
interpreting front panel LEDs, 17-1
interpreting IPX SAP interface statistics, 13-8, 13-9, 14-13, 14-14
interval start
Ethernet interface statistical parameters, 19-4
intra-area routes
IP global configuration parameters, 9-14
invalid entry
permanent, definition, 6-20
invalid flows from upstream
DVMRP multicast forwarding cache parameters, 9-90
IGMP local multicast forwarding cache parameters, 9-79
invalid routes received
DVMRP interface statistical parameters, 9-82
IP
creating OSPF summaries, 11-18, 11-19, 11-20
creating OSPF virtual links, 11-14, 11-16
creating RIP trusted neighbors, 10-7, 10-8
displaying OSPF links, 11-24
displaying OSPF neighbors, 11-25
displaying OSPF statistics, 11-21
DVMRP configuration, 9-57
interface configuration, 9-6
modifying OSPF areas, 11-9
multicast forwarding, 9-50
multicast routing, 9-51
multicast statistics, 9-72
multicast, overview, 9-50
OSPF area creation, 11-5

OSPF global configuration, 11-3
RIP configuring interfaces, 10-4
RIP global configuration, 10-1
RIP statistics, 10-12, 10-13
searching the OSPF link state database, 11-27, 11-32
Searching the routing table, 9-68
IP access list parameters
access list name, 9-23, 9-26
access rule index, 9-23, 9-26
access type, 9-24, 9-26
destination subnet, 9-26
protocol ID, 9-26
TCP established, 9-27
TCP/UDP destination port, 9-27
TCP/UDP source port, 9-27
IP access rules
creating rules for filtering traffic between subnets, 9-30
filtering traffic between subnets example, 9-30
filtering web traffic example, 9-29
IP address
ARP cache search parameters, 9-72
configuring SNMP communities, 2-21
DVMRP interface parameters, 9-60
IGMP interface parameters, 9-55
IGMP interface statistical parameters, 9-75
IP routing table search parameters, 9-69
IP static ARP parameters, 9-46
OSPF interface parameters, 11-11
OSPF link parameters, 11-24
OSPF neighbors parameters, 11-26
RIP statistical parameters, 10-11, 10-13
static multicast session configuration parameters, 16-16
static multicast session parameters, 16-18
VRRP configuration parameters, 9-98
VRRP statistical parameters, 9-101
IP address mask
DVMRP interface parameters, 9-60
IGMP interface parameters, 9-55
IGMP interface statistical parameters, 9-75
IP and IPX router, 1-28
IP ARP
searching ARP cache, 9-71
IP forward datagrams
IP routing global statistics, 9-64
IP fragmentation creates
IP routing global statistics, 9-65
IP fragmentation failures, 9-65
IP fragmentation OKs
IP routing global statistics, 9-65
IP Global Configuration Dialog Box, 9-49
IP global configuration parameters
BOOTP/DHCP relay agent, 9-13
high-preference static routes, 9-14
intra-area routes, 9-14
IP multicast forwarding, 9-13
IP routing, 9-13
IP source routing, 9-13
limit proxy ARP to same network, 9-13
local routes, 9-14
low-preference static routes, 9-14
maximum number of ARP cache entries, 9-13
maximum number of routes, 9-13
OSPF external routes, 9-14
OSPF inter-area routes, 9-14
RIP routes, 9-14
route preference by protocol, 9-14
use default route for proxy ARP, 9-13
VRRP, 9-13
IP global routing
configuring, 9-11
IP global routing statistics
displaying, 9-62, 9-71
IP in address errors
IP routing global statistics, 9-64
IP in delivers
IP routing global statistics, 9-64
IP in discards
IP routing global statistics, 9-64
IP in header errors
IP routing global statistics, 9-63
IP in receives
IP routing global statistics, 9-63
IP in unknown protocols
IP routing global statistics, 9-64
IP interface
creating, 9-4, 9-9
IP interface access list rules
creating, 9-21
IP interface access lists
configuring, 9-17
IP interface parameters
interface, 9-8
IP interfaces
configuring, 9-6
IP multicast
overview, 9-50
IP multicast forward datagrams
IP routing global statistics, 9-67
IP multicast forwarding
IP global configuration parameters, 9-13
IP multicast in discard
IP routing global statistics, 9-67
IP multicast in receives
IP routing global statistics, 9-68
IP out discards

, 9-65
IP out no routes
IP routing global statistics, 9-65
IP out requests
IP routing global statistics, 9-64
IP reassembly failures
IP routing global statistics, 9-65
IP reassembly OKs
IP routing global statistics, 9-65
IP reassembly required
IP routing global statistics, 9-65
IP reassembly timeout
IP routing global statistics, 9-65
IP routing
add IP interface parameters, 9-8
creating a BOOTP/DHCP server entry, 9-46, 9-47
IP global configuration parameters, 9-13
statistics, 9-61
IP routing discards
IP routing global statistics, 9-65
IP routing global statistics
BOOTP/DHCP in discards, 9-68
BOOTP/DHCP in hops exceeded, 9-68
BOOTP/DHCP in requests, 9-68
BOOTP/DHCP in responses, 9-68
BOOTP/DHCP out requests, 9-68
BOOTP/DHCP out responses, 9-68
ICMP in address mask reply, 9-66
ICMP in address mask requests, 9-66
ICMP in destination unreachable, 9-66
ICMP in echo replys, 9-66
ICMP in echo requests, 9-66
ICMP in errors, 9-66
ICMP in messages, 9-66
ICMP in parameter problems, 9-66
ICMP in redirects, 9-66
ICMP in source quenches, 9-66
ICMP in time exceeds, 9-66
ICMP in timestamp replys, 9-66
ICMP in timestamp requests, 9-66
ICMP out address mask reply, 9-67
ICMP out address mask requests, 9-67
ICMP out destination unreachable, 9-66
ICMP out echo reply, 9-67
ICMP out echo requests, 9-67
ICMP out errors, 9-66
ICMP out messages, 9-66
ICMP out parameter problems, 9-67
ICMP out redirects, 9-67
ICMP out source quenches, 9-67
ICMP out time exceeded, 9-66
ICMP out timestamp reply, 9-67
ICMP out timestamp request, 9-67
IP forward datagrams, 9-64
IP fragmentation creates, 9-65
IP fragmentation failures, 9-65
IP fragmentation OKs, 9-65
IP in address errors, 9-64
IP in delivers, 9-64
IP in discards, 9-64
IP in header errors, 9-63
IP in receives, 9-63
IP in unknown protocols, 9-64
IP multicast forward datagrams, 9-67
IP multicast in discard, 9-67
IP multicast in receives, 9-68
IP out discards, 9-65
IP out no routes, 9-65
IP out requests, 9-64
IP reassembly failures, 9-65
IP reassembly OKs, 9-65
IP reassembly required, 9-65
IP reassembly timeout, 9-65
IP routing discards, 9-65
UDP in datagrams, 9-67
UDP in errors, 9-67
UDP in no ports, 9-67
UDP out datagrams, 9-67
IP routing search table
deleting local entries from routing table, 9-70
IP routing statistics, 9-61
IP routing table
searching, 9-68
IP routing table search parameters
interface, 9-69
IP address, 9-69
source, 9-69
IP routing table statistical parameters
current number of routes, 9-71
peak number of routes, 9-71
RIP queries, 9-71
RIP route changes, 9-71
total routes added, 9-71
total routes deleted, 9-71
IP routing table statistics
examining, 9-70
IP source routing
IP global configuration parameters, 9-13
IP static ARP parameters
IP address, 9-46
MAC address, 9-46
IP static route
creating static ARP entries, 9-45
IP static route parameters
cost, 9-44
mask, 9-44
network address, 9-44

next-hop address, 9-44
preference, 9-44
IP static routes
creating, 9-43
IPX, C-1
creating static routes, 12-9, 12-10, 12-12
creating static services, 12-13, 12-14, 12-16
datagram structure, 12-2
deleting static routes, 12-12
deleting static service, 12-16, 12-17
examining the route table, 12-21
examining the service table, 12-24
global statistics, 12-18, 12-19
interface configuration, 12-5, 12-9
modifying IPX RIP filters, 13-3, 13-7, 13-8
modifying static routes, 12-13
modifying static services, 12-17
network number, 12-1
node number, 12-1
RIP interfaces, 13-1
routing table statistics, 12-22
searching the route table, 12-20
searching the service table, 12-23
socket number, 12-1
IPX datagram fields
checksum, 12-2
destination network, 12-3
destination node, 12-3
destination socket, 12-3
packet length, 12-2
packet type, 12-3
source network, 12-3
source node, 12-3
source socket, 12-3
transport control, 12-2
IPX datagram structure, 12-2
IPX forward datagrams
IPX global parameters, 12-19
IPX global parameters, 12-4, 12-5, 12-9
in max hops exceeded, 12-19
IPX forward datagrams, 12-19
IPX in checksum errors, 12-19
IPX in delivery, 12-19
IPX in discards, 12-19
IPX in header errors, 12-19
IPX in ping replies, 12-19
IPX in ping request, 12-19
IPX in receives, 12-19
IPX in unknown sockets, 12-19
IPX Netbios receives, 12-19
IPX out discards, 12-19
IPX out no routes, 12-19
IPX out packets, 12-19
IPX out ping replies, 12-19
IPX out ping requests, 12-19
IPX out requests, 12-19
maximum number of services, 12-5
IPX in checksum errors
IPX global parameters, 12-19
IPX in delivery
IPX global parameters, 12-19
IPX in discards
IPX global parameters, 12-19
IPX in header errors
IPX global parameters, 12-19
IPX in ping replies
IPX global parameters, 12-19
IPX in ping request
IPX global parameters, 12-19
IPX in receives
IPX global parameters, 12-19
IPX in unknown sockets
IPX global parameters, 12-19
IPX interface
admin state, 12-8
frame type, 12-8
interface, 12-8
network address, 12-8
node address, 12-8
RIP, 12-8
ticks, 12-8
type 20 packet propagation, 12-9
VLAN, 12-8
IPX interface MIbs, C-1
IPX Netbios receives
IPX global parameters, 12-19
IPX out discards
IPX global parameters, 12-19
IPX out no routes
IPX global parameters, 12-19
IPX out packets
IPX global parameters, 12-19
IPX out ping replies
IPX global parameters, 12-19
IPX out pint requests
IPX global parameters, 12-19
IPX out requests
IPX global parameters, 12-19
IPX overview, 12-1
IPX RIP filter
suppress advertising of all networks example, 13-5, 13-6
IPX RIP filter parameters
direction, 13-5
end network, 13-4
filter/suppress, 13-5
hops, 13-5

interface, 13-4
precedence, 13-4
start network, 13-4
ticks, 13-5
IPX RIP filters
creating, 13-3, 13-7, 13-8
IPX RIP filters, modifying, 13-3, 13-7, 13-8
IPX RIP interface statistics
displaying, 7-1
IPX route table
examining, 12-21
IPX route table parameters
hops, 12-22
interface, 12-21
network, 12-21
next-hop MAC address, 12-22
source, 12-21
ticks, 12-22
TTL, 12-21
IPX route table search, 12-20
IPX route table statistics
examining, 12-22
IPX router
configuring, 12-4, 12-5
IPX routing
IPX routing, 12-4
IPX routing global statistics, displaying, 12-18, 12-19
IPX routing table search parameters
interface, 12-21
network number, 12-21
source, 12-21
IPX routing table statistics
current number of routes, 12-22
peak number of routes, 12-22
route add failures, 12-22
IPX SAP filter parameters
direction, 14-6
filter/suppress, 14-6
hops, 14-6
interface, 14-5
name, 14-5
precedence, 14-5
type, 14-6
IPX SAP filters
creating, 14-3, 14-4
filtering all services except NDS example, 14-11
suppress advertising of print servers example, 14-7
IPX SAP interface parameters
aging interval multiplier, 14-2
get nearest server reply, 14-3
get nearest server reply delay, 14-3
interface, 14-2
mode, 14-3
network number, 14-2
periodic update interval, 14-2
triggered updates, 14-2
use interpacket gap, 14-2
use max packet size, 14-2
IPX SAP interface statistical parameters
bad packets received, 13-9, 14-14
GNS requests received, 14-14
GNS responses sent, 14-14
interface, 13-8, 14-13
network number, 13-9, 14-13
non-triggered updates sent, 13-9, 14-14
requests received, 13-9, 14-14
state, 13-8, 14-13
updates received, 13-9, 14-14
IPX SAp interface statistical parameters
triggered updates sent, 13-9, 14-14
IPX SAP interface statistics
interpreting, 13-8, 13-9, 14-13, 14-14
IPX SAP interfaces
configuring, 14-1
IPX SAP network filter parameters
direction, 14-10
filter/suppress, 14-10
hops, 14-10
interface, 14-9
net, 14-9
precedence, 14-9
type, 14-10
IPX SAP network filters
creating, 14-8, 14-12
IPX service table
examining, 12-24
searching, 12-23
IPX service table parameter
hops, 12-25
interface, 12-25
network, 12-25
next-hop MAC address, 12-25
node, 12-25
socket, 12-25
source, 12-25
TTL, 12-25
type, 12-25
IPX service table parameters
name, 12-25
IPX service table search parameter
service name, 12-24
service type, 12-24
IPX service table search parameters
interface, 12-24
source, 12-24
IPX static route
hops, 12-11

interface, 12-11
network, 12-11
next-hop node, 12-11
ticks, 12-11
IPX static route parameters, 12-11
IPX static routes
creating, 12-10, 12-12
deleting, 12-12
modifying, 12-13
IPX static service parameter
hops, 12-15
interface, 12-15
network, 12-15
next-hop node, 12-15
node, 12-15
service name, 12-15
socket, 12-15
type, 12-15
IPX static service parameters, 12-15
IPX static services
creating, 12-14, 12-16
IPX syntax example, 12-1
IRDP, 9-106
enabling on an interface, 9-106
IRDP overview, 9-106
IRDP parameters
adv. address, 9-107
advertisement life time, 9-107
interface, 9-107
IRDP state, 9-107
max. advertisement interval, 9-107
minimum advertisement interval, 9-107
network address, 9-107
preferences, 9-107
IRDP state
IRDP parameters, 9-107

## *J*

jabbers
Ethernet interface statistical parameters, 19-7

## *K*

key
OSPF interface parameters, 11-11
known mode
non-VLAN switch port parameters, 5-28
switch port configuration parameters, 5-29

## *L*

L2 frame count
frame forwarding statistical parameters, 18-6
L3 drop frames
frame forwarding statistical parameters, 18-6
L3 frame cache hits
frame forwarding statistical parameters, 18-5
L3 slow path frames
frame forwarding statistical parameters, 18-5
L3 total (T2)
frame forwarding statistical parameters, 18-5
LAN router
configuration, 9-3
last change
LDAP statistics, 9-113
Layer 2
event log, 17-6
redundant switch matrix and controller module, 1-21
shutdown log, 17-6
Layer 2 Fast Ethernet modules
20-port 10/100BASE-TX, 1-10
Layer 2 Gigabit Ethernet modules, 1-11
Layer 2 routing
overview, 1-30
Layer 2 switching, 1-29
Layer 2/3 routing example, 1-30
Layer 3 (learned) traffic routing
overview, 1-30
Layer 3 (not learned) traffic routing
overview, 1-30
Layer 3 cache configuration
age interval, 18-3
aging, 18-3
hash mode, 18-3
maximum entries, 18-3
Layer 3 dynamic intelligent multicasting, 16-4
Layer 3 forwarding cache
displaying, 18-9
Layer 3 forwarding cache (FE) parameters
aged entries, 18-11
current entries, 18-11
duplicate add attempts, 18-11
entries removed due to route changes, 18-11
entries removed due to route deletes, 18-11
failed add attempts, 18-11
lookup hits, 18-11
lookup levels, 18-11
lookup misses, 18-11
memory use in bytes, 18-11
mode, 18-11
PRE, 18-11
total entries, 18-11
type, 18-11
Layer 3 overview, 16-4
Layer 3 route cache search parameters

comparison value, 18-8
destination address, 18-7
destination port, 18-8
PRE, 18-8
protocol, 18-7
rule number, 18-8
source address, 18-7
source port, 18-8
VLAN, 18-8
Layer 3 routing
overview, 1-29
LDAP
configuring, 9-109
configuring settings, 9-110, 9-112
configuring statistics, 9-113, 9-114
event class parameters, 17-18
settings, 9-109
LDAP configuration parameters
primary server IP address, 9-111
primary server port, 9-111
search base, 9-111
secondary server IP address, 9-111
secondary server port, 9-111
LDAP statistics
consumer signal, 9-114
last change, 9-113
producer signal, 9-114
learned entries
delete invalid learned entries, 6-14
learning state (spanning tree bridge port), 4-22
LEDs
port (10/100 module), 17-2
LGMP client configuration parameters
enable state, 16-32
intelligent multicast session statistics, 16-32
LGMP clients, 16-32
LGMP message reception statistics, 16-32
LGMP client display per VLAN parameters
intelligent multicast session statistics, 16-35
LGMP message reception statistics, 16-34
VLAN, 16-34
LGMP client, configuring
configuring/viewing a LGMP client, 16-32, 16-33
LGMP clients
LGMP client configuration parameters, 16-32
LGMP message reception statistics
LGMP client configuration parameters, 16-32
LGMP client display per VLAN parameters, 16-34
LGMP server display per VLAN parameters, 16-29
LGMP message statistics
LGMP server configuration parameters, 16-25
LGMP message transmission statistics
LGMP server configuration parameters, 16-26
LGMP messages transmission statistics
LGMP server display per VLAN parameters, 16-29
LGMP server, 16-27
LGMP server configuration, 16-26, 16-27, 16-28, 16-30
LGMP server configuration parameters
enable state, 16-25
intelligent multicast session statistics, 16-26
LGMP message reception statistics, 16-25
LGMP message transmission statistics, 16-26
LGMP servers, 16-25
proxy mode, 16-25
robustness variable, 16-25
router report time, 16-25
server ID priority, 16-25
LGMP server display per VLAN parameters
intelligent multicast session statistics, 16-29
LGMP message reception statistics, 16-29
LGMP messages transmission statistics, 16-29
state, 16-29
VLAN, 16-28
LGMP servers
LGMP server configuration parameters, 16-25
limit proxy ARP to same network
IP global configuration parameters, 9-13
link state database, 11-27, 11-32
link state database search parameters
area ID, 11-29
router ID, 11-29
type, 11-29
links
switch port parameter, 5-37
listening state (spanning tree bridge port), 4-22
load MIB
overview, 1-17, C-4
Load Share Function, 4-32
local ext type
OSPF global configuration parameters, 11-4
local routes
IP global configuration parameters, 9-14
log ID
event and shutdown log entries, 17-14
logging into
Web Agent, 2-9
lookup hits
forwarding cache (FE) parameters, 18-11
lookup levels
forwarding cache (FE) parameters, 18-11
lookup misses
forwarding cache (FE) parameters, 18-11
low shutdown temperature
temperature threshold parameter, 17-4
lower warning temperature
temperature threshold parameter, 17-4
low-preference static routes

IP global configuration parameters, 9-14
LS ID
LSA detail, 11-32
OSPF link state database parameter, 11-30
LSA checksum sum
OSPF statistical parameters, 11-22
LSA chksum sum
OSPF statistical parameters, 11-23
LSA detail
age, 11-32
area, 11-32
attached router ID 1 & 2, 11-32
checksum, 11-32
LS ID, 11-32
network mask, 11-32
router ID, 11-32
sequence, 11-32
type, 11-32
LSAs
OSPF statistical parameters, 11-23

## *M*

MAC Address
search, 6-16
MAC address
address forwarding table parameters, 6-19
AppleTalk ARP cache table statistics, 15-32
filtering, 6-16
IP static ARP parameters, 9-46
multicast session parameters, 16-12
static multicast session configuration parameters, 16-16
static multicast session parameters, 16-18
switch port parameter, 5-37
MAC address value
adding, 6-21
MAC format
add IP interface parameters, 9-8
managing buffers and queues, 20-2, 20-7
mask
add IP interface parameters, 9-8
IP static route parameters, 9-44
OSPF summaries parameters, 11-19
master
OSPF neighbors parameters, 11-26
max age
spanning tree bridge level parameters, 4-19
max packets per second
port mirroring information parameters, 19-10
max. packets per secondl
mirror port configuration parameters, 19-13
max.advertisement interval
IRDP parameters, 9-107
maximum entries
Layer 3 cache configuration, 18-3
maximum groups
IGMP interface parameters, 9-56
maximum number of ARP cache entries
IP global configuration parameters, 9-13
maximum number of paths
OSPF global configuration parameters, 11-4
maximum number of routes
DVMRP parameters, 9-59
IP global configuration parameters, 9-13
maximum number of routes, 12-5
maximum number of services
IPX global parameters, 12-5
MC-option
OSPF neighbors parameters, 11-27
MD5 key ID
OSPF interface parameters, 11-12
OSPF virtual link parameters, 11-16
memory
buffer detailed configuration parameters, 20-5
memory use in bytes
forwarding cache (FE) parameters, 18-11
metric
AppleTalk interface parameters, 15-6
AppleTalk route table statistics, 15-29
DVMRP interface statistical parameters, 9-82
MIB groups supported, C-1
MIBs
AppleTalk, C-4
bridge MIBs, C-2
DVMRP, C-4
IEEE 802.3 MAU, C-1
IEEE 802.3 statistics group, C-2
IGMP, C-3
IP forwarding/routing table, C-4
IP interface, C-3
IP version 4.0, C-3
OSPF v2.0, C-2
policy capability MIB for LDAP, C-4
private IPX interface MIBs, C-1
Prominent, C-1
RIP v1 and v2, C-2
RMON, C-2
SNMPv2, C-2
VRRP, C-3
minimum adv. interval
IRDP parameters, 9-107
minutes
summer time hours configuration, 3-8
mirror port
configuring
configuring a mirror port, 19-8, 19-13, 19-19

port mirroring information parameters, 19-10
RMON mirror port configuration parameters, 19-11
switch port configuration parameters, 5-29
mirror port configuration parameters
max. packets per second, 19-13
mode
forwarding cache (FE) parameters, 18-11
IPX SAP interface parameters, 14-3
RIP interface parameters, 10-4
spanning tree bridge level parameters, 4-19
modem
connecting, 2-35
modem configuration string parameters
&D0, 2-38
CD follows carrier, 2-38
E0, 2-39
S0=1, 2-38
software flow control, 2-39
modify IPX static routes, 12-13
modifying DVMRP interface information, 9-59
modifying IGMP interfaces, 9-55
Modifying OSPF Summaries, 11-20
modifying OSPF virtual links, 11-17
Modifying the DVMRP Global Configuration Using the CLI, 9-61
module features, 1-10
modules & ports, 4-45, 5-12, 5-17, 5-23, 5-24, 5-33, 5-36, 5-37
monitoring switch performance
IP routing statistics, 9-61
OSPF, 11-21
Monitoring the Forwarding Cache Statistics, 18-4
month
summer time hours configuration, 3-8
multicast forwarding
description, 9-50
multicast forwarding cache
displaying, 9-89
multicast packets
Ethernet interface statistical parameters, 19-5
multicast protocol
add IP interface parameters, 9-9
multicast routing
description, 9-51
multicast session client port parameters
application, 16-14
port, 16-14
multicast session parameters
application, 16-12
client port, 16-12
MAC address, 16-12
session ID, 16-12
type, 16-12
VLAN, 16-12
multicast statistics
IP, 9-72
multi-gigabit connections example, 4-28
multilayer Fast Ethernet modules
20-port 10/100BASE-TX, 1-10
multi-link trunk groups
features, 4-29
multinetting, 9-14, 12-5

## *N*

name
AppleTalk NBP filter parameters, 15-17
AppleTalk NBP table parameters, 15-35
AppleTalk zone filter parameters, 15-21
AppleTalk zone table statistics, 15-33
IPX SAP filter parameters, 14-5
IPX service table parameter, 12-25
spanning tree bridge port parameters, 4-21
switch port parameter, 5-37
NBP filter
adding interfaces, 15-19, 15-20, 15-24
deleting interfaces, 15-19, 15-20, 15-24
editing, 15-18
neighbor DVMRP routers
DVMRP interface statistical parameters, 9-82
neighbor is SNMP manageable
DVMRP neighbor routers, 9-84
neighbor network address
DVMRP neighbor routers, 9-83
neighbor querier timeout in sec
IGMP interface statistical parameters, 9-76
neighbor querier timeout interval
IGMP interface parameters, 9-56
neighbor received probe from this router
DVMRP neighbor routers, 9-84
neighbor supports generation ID function
DVMRP neighbor routers, 9-84
neighbor supports MTRACE requests
DVMRP neighbor routers, 9-84
neighbor supports prune function
DVMRP neighbor routers, 9-84
net
IPX SAP network filter parameters, 14-9
NetBIOS UDP rebroadcast
add IP interface parameters, 9-9
network
IPX route table parameter, 12-21
IPX service table parameter, 12-25
IPX static route, 12-11
IPX static service parameter, 12-15
network address
add IP interface parameters, 9-8

DVMRP interface statistical parameters, 9-82
IP static route parameters, 9-44
IPX interface, 12-8
IRDP parameters, 9-107
OSPF summaries parameters, 11-19
RIP interface parameters, 10-4
network mask
LSA detail, 11-32
network number
AppleTalk interface parameters, 15-7
AppleTalk interface statistics, 15-28
AppleTalk static route, 15-12
IPX routing table search parameters, 12-21
IPX SAP interface parameters, 14-2
IPX SAP interface statistical parameters, 13-9, 14-13
network range
AppleTalk ARP cache table statistics, 15-32
AppleTalk interface statistics, 15-28
AppleTalk route table statistics, 15-29
AppleTalk zone table statistics, 15-33
network range end
AppleTalk interface parameters, 15-7
AppleTalk static route, 15-12
network range start
AppleTalk interface parameters, 15-7
AppleTalk static route, 15-12
new client ports added
IGMP snooping, 16-21
new router ports added
IGMP snooping, 16-21
new sessions created
IGMP snooping, 16-21
next hop
AppleTalk route table statistics, 15-29
next probe message in sec
DVMRP interface statistical parameters, 9-82
next pruned downstream interface to timeout
DVMRP multicast forwarding cache parameters, 9-91
next query request in sec
IGMP interface statistical parameters, 9-75
next-hop address
IP static route parameters, 9-44
next-hop MAC address
IPX route table parameter, 12-22
IPX service table parameter, 12-25
next-hop node
IPX static route, 12-11
IPX static service parameter, 12-15
no client
AppleTalk global statistics, 15-26
no route
AppleTalk global statistics, 15-26
node
AppleTalk ARP cache table statistics, 15-32
AppleTalk interface parameters, 15-7
AppleTalk interface statistics, 15-28
AppleTalk static route, 15-13
IPX service table parameter, 12-25
IPX static service parameter, 12-15
node address
IPX interface, 12-8
none
SNMP access level, 2-22
non-tagged access mode,definition, 1-10
non-triggered updates sent
IPX SAP interface statistical parameters, 13-9, 14-14
RIP statistical parameters, 10-11, 10-13
non-VLAN switch port parameters, configuring
3Com mapping table, 5-28
allow learning, 5-27
hunt group, 5-27
known mode, 5-28
spanning tree, 5-27
N-option
OSPF neighbors parameters, 11-27
normal
SNMP security level, 2-22
normal-priority traffic, 20-1
nstalling the HTTP Documentation Server, -xix
number of current groups
IGMP interface statistical parameters, 9-76
number of routes
IPX routing table statistic, 12-22
number of triggered routes
DVMRP routing statistical parameters, 9-85
number of valid routes
DVMRP routing statistical parameters, 9-85

## *O*

one-time summer time hours configuration, 3-9
end, 3-9
start, 3-9
Online documentation
adding files to a Web server, -xxi
getting updated online documentation, -xxii
installing, -xix
installing the HTTP server, -xix
starting the HTTP server, -xx
online documentation, -xviii
Online Help, -xix
Online help, -xix
accessing help files from the server, -xx
adding files to a Web server, -xxi
getting updated help files, -xxii
Open Trunk technology features, 1-16
OpenTrunk technology,overview, 1-16

OPQ option
OSPF neighbors parameters, 11-27
originate LSA count
OSPF statistical parameters, 11-22
OSPF
add IP interface parameters, 9-9
creating areas, 11-5
creating summaries, 11-18, 11-19, 11-20
creating virtual links, 11-14, 11-16
displaying links, 11-24
displaying neighbors, 11-25
event class parameters, 17-18
monitoring switch performance, 11-21
OSPF global configuration parameters, 11-4
searching the link state database, 11-27, 11-32
OSPF area parameters
area ID, 11-6
area type, 11-6
stub metric, 11-6
translate 7 into 5, 11-6
type 3 ASE filter, 11-6
OSPF areas
deleting, 11-7, 11-8
OSPF external routes
IP global configuration parameters, 9-14
OSPF global configuration
configuring, 11-3
OSPF global configuration parameters
AS border route, 11-4
auto-creation of virtual links, 11-4
local ext type, 11-4
maximum number of paths, 11-4
OSPF, 11-4
RIP ext type, 11-4
router ID, 11-4
SPF hold time, 11-4
SPF suspend, 11-4
static ext type, 11-4
static low ext type, 11-4
OSPF inter-area routes
IP global configuration parameters, 9-14
OSPF interface parameters
area, 11-11
authentication, 11-11
cost, 11-11
dead interval, 11-11
DR priority, 11-11
hello interval, 11-11
interface, 11-11
IP address, 11-11
key, 11-11
MD5 key ID, 11-12
poll interval, 11-11
retransmit interval, 11-11
transit delay, 11-11
OSPF interfaces
modifying, 11-9
OSPF link parameters
area ID, 11-24
BDR address, 11-24
DR address, 11-24
DR router ID, 11-24
IP address, 11-24
state, 11-24
type, 11-24
OSPF link state database parameter
age, 11-31
area ID, 11-30
checksum, 11-31
detail link, 11-30
LS ID, 11-30
router ID, 11-31
sequence, 11-31
type, 11-30
OSPF link state database search parameters
area ID, 11-29
router ID, 11-29
type, 11-29
OSPF neighbors parameters
BDR choice, 11-27
DD number, 11-26
DR choice, 11-27
DR priority, 11-27
E-option, 11-27
IP address, 11-26
master, 11-26
MC-option, 11-27
N-option, 11-27
OPQ-option, 11-27
router ID, 11-26
state, 11-26
T-option, 11-27
OSPF packet tracing
enabling, 17-7, 17-12
OSPF state
OSPF statistical parameters, 11-22
OSPF statistical parameters
area ID, 11-23
AS border Rtrs, 11-23
border Rtrs, 11-23
external LSA count, 11-22
LSA checksum sum, 11-22
LSA chksum sum, 11-23
LSAs, 11-23
originate LSA count, 11-22
OSPF state, 11-22
OSPF version, 11-22

receive new LSA count, 11-22
router ID, 11-22
SPF runs, 11-23
OSPF statistics
displaying, 11-21
OSPF summaries parameters
advertisement, 11-19
area, 11-19
mask, 11-19
network address, 11-19
OSPF version
OSPF statistical parameters, 11-22
OSPF virtual link parameters
area, 11-15
authentication, 11-16
authentication key, 11-16
dead interval, 11-16
hello interval, 11-15
MD5 key ID, 11-16
retransmit interval, 11-15
router ID, 11-15
transit delay, 11-15
OSPF virtual links
deleting, 11-16
modifying, 11-17
overflow drops
buffer management table parameters, 20-6
oversize packets
Ethernet interface statistical parameters, 19-6
overview, 1-16
ATM, 1-7
intelligent multicasting, 16-4
overview of Layer 2 traffic routing, 1-30
overview of Layer 3 (learned) traffic routing, 1-30
overview of Layer 3 (not learned) traffic routing, 1-30
overview of Layer 3 routing, 1-29
owner
AppleTalk route table statistics, 15-29

## *P*

packet length
IPX datagram fields, 12-2
packet tracing
enabling, 17-7, 17-12
packet type
IPX datagram fields, 12-3
packets
Ethernet interface statistical parameters, 19-4
packets forwarded through cache entry
DVMRP multicast forwarding cache parameters, 9-90
IGMP local multicast forwarding cache parameters, 9-79
parity
console serial port settings, 2-34
path cost
spanning tree bridge port information parameters, 4-23
payload protocol type
DVMRP upstream source parameters, 9-92
peak number of routes
AppleTalk route table statistics, 15-31
IP routing table statistical parameters, 9-71
IPX routing table statistic, 12-22
peak number of zones
AppleTalk zone table statistics, 15-34
PER VLAN SPANNING TREE, 1-18
percent cache hits
frame forwarding statistical parameters, 18-5
percent drops
frame forwarding statistical parameters, 18-6
percent slow path
frame forwarding statistical parameters, 18-5
performing a system reset, 3-16
periodic update interval
IPX SAP interface parameters, 14-2
permanent
address forwarding table, persistence parameters, 6-22
invalid entry, 6-20
persistence entry, 6-20
persistence
address forwarding table parameters, 6-20
persistence entry
ageout, definition, 6-20
permanent, definition, 6-20
physical port buffers
buffer management parameters, 20-4
piggyback port
port mirroring information parameters, 19-10
port mirroring parameter, 19-12
poll interval
OSPF interface parameters, 11-11
port
address forwarding table parameters, 6-19
multicast session client port parameters, 16-14
RMON mirror port configuration parameters, 19-11
router port display parameters, 16-9
spanning tree bridge port parameters, 4-21
switch port parameter, 5-37
VLAN switch port table parameters, 4-12
port density, 1-3, 1-5, 1-6
port LED (10/100 module)
behavior, 17-2
port mirror, 19-8
port mirroring information parameters, 19-9

configure source, 19-9
max packets per second, 19-10
mirror port, 19-10
piggyback port, 19-10
sampler type, 19-10
source port, 19-9
port mirroring parameters, 19-13
port name
gigabit port parameters, 5-15
VLAN switch port table parameters, 4-12
port PACE priority
10/100 port parameter, 5-22
gigabit port parameters, 5-16
port VLAN
Cisco Catalyst 5000 parameters, 5-30
switch port configuration parameters, 5-28
switch port parameter, 5-37
port-based VLANs, 4-2
power supply
power system statistical parameters, 3-14
power system statistical parameters
current power available, 3-14
power supply, 3-14
status, 3-14
total system power, 3-14
type, 3-14
power system statistics
displaying, 3-13
power-up/reset image
CPU redundancy configuration, 7-18
PPP console
configuring, 2-36
configuring a network mask, 9-116
configuring an IP address, 9-116
PPP console settings
baud rate, 2-34
flow control, 2-34
PPP console static route
configuring, 9-115
PPP serial port console, 2-42
regaining access to the CLI, 2-40
PRE
forwarding cache (FE) parameters, 18-11
Layer 3 route cache search parameters, 18-8
precedence
IPX RIP filter parameters, 13-4
IPX SAP filter parameters, 14-5
IPX SAP network filter parameters, 14-9
preference
IP static route parameters, 9-44
preferences
IRDP parameters, 9-107
primary controller
replacing, 7-9
primary server
RADIUS configuration parameters, 2-30
primary server IP address
LDAP configuration parameters, 9-111
primary server port
LDAP configuration parameters, 9-111
priority
address forwarding table parameters, 6-19
spanning tree bridge level parameters, 4-19
spanning tree bridge port information parameters, 4-23
VRRP configuration parameters, 9-98
priority queuing,definition, 1-10
priority threshold
buffer management table parameters, 20-6
probe message received
DVMRP global statistical parameters, 9-80
probe messages transmitted
DVMRP global statistical parameters, 9-80
process leave packets
IGMP interface parameters, 9-56
producer signal
LDAP statistics, 9-114
Prominent MIBs, C-1
protocol
Layer 3 route cache search parameters, 18-7
protocol event log
configuring, 17-7, 17-12
protocol event log settings
debug, 17-12
error, 17-11
fault, 17-11
info, 17-11
trace, 17-12
warning, 17-11
protocol ID
IP access list parameters, 9-26
proxy ARP
add IP interface parameters, 9-9
IP global configuration parameters, 9-13
proxy mode
LGMP server configuration parameters, 16-25
prune expiration
DVMRP downstream link parameters, 9-92
prune expiration time
upstream prune information, 9-91
prune messages received
DVMRP global statistical parameters, 9-80
prune messages transmitted
DVMRP global statistical parameters, 9-81
purge TTL
RIP global configuration parameters, 10-2

# *Q*

query messages received
IGMP interface statistical parameters, 9-76
query messages transmitted
IGMP interface statistical parameters, 9-76
query request interval
IGMP interface parameters, 9-56
query response interval
IGMP interface parameters, 9-56
queues
managing, 20-2, 20-7
service ratio, 20-1

# *R*

RADIUS client
configuring, 2-29, 2-31
RADIUS configuration parameters
Cajun-Service-Type required, 2-31
enable state, 2-30
group, 2-31
primary server, 2-30
realm, 2-30
retry number, 2-31
retry time, 2-31
secondary server, 2-30
shared secret, 2-30
source IP address, 2-30
UDP port, 2-31
RADIUSsecondary server
shared secret, 2-30
rate limit burst size
10/100 port parameter, 5-22
rate limit mode
10/100 port parameter, 5-22
rate limit rate
10/100 port parameter, 5-22
read-only
SNMP access level, 2-21
read-write
SNMP access level, 2-21
read-write with security level set to admin
SNMP access level, 2-22
realm
RADIUS configuration parameters, 2-30
receive new LSA count
OSPF statistical parameters, 11-22
receive version
RIP interface parameters, 10-5
recurring
summer time hours configuration, 3-7
redundant CPU
configuring, 7-11
redundant element, 7-5
configuring, 7-10
Related Documentation, -xviii
related documents, -xviii
Remote Authentication Dial-In User Service (RADIUS) Client Support, 8-1
replacing the primary controller, 7-9
report messages received
DVMRP global statistical parameters, 9-80
report messages transmitted
DVMRP global statistical parameters, 9-80
reporting router
DVMRP route table parameters, 9-86
reporting router interface
DVMRP route table parameters, 9-86
requests received
IPX SAP interface statistical parameters, 13-9, 14-14
resetting the switch, A-8
Resetting the Switch Using the Web Agent, A-8
resource
event class parameters, 17-17
retransmit interval
OSPF interface parameters, 11-11
OSPF virtual link parameters, 11-15
retry number
RADIUS configuration parameters, 2-31
retry time
RADIUS configuration parameters, 2-31
RIP
add IP interface parameters, 9-9
creating trusted RIP neighbors, 10-7, 10-8
event class parameters, 17-18
IPX interface, 12-8
RIP, 12-4
trusted neighbors, 10-7, 10-8
RIP ext type
OSPF global configuration parameters, 11-4
RIP global configuration, 10-1
RIP global configuration parameters
global RIP, 10-2
purge TTL, 10-2
triggered updates, 10-3
update pkt delay, 10-3
update timer, 10-2
RIP interface parameters
auth key, 10-6
auth type, 10-6
default metric, 10-5
default route, 10-5
interface, 10-4
mode, 10-4
network address, 10-4
receive version, 10-5

split horizon, 10-5
version, 10-5
RIP interfaces
configuring, 10-4
RIP packet tracing
enabling, 17-7, 17-12
RIP queries
IP routing table statistical parameters, 9-71
RIP route changes
IP routing table statistical parameters, 9-71
RIP routes
IP global configuration parameters, 9-14
RIP statistical parameters
bad packets received, 10-11, 10-13
bad routes received, 10-11, 10-13
interface, 10-13
IP address, 10-11, 10-13
non-trigger updates sent, 10-11, 10-13
state, 10-13
triggered updates sent, 10-13
updates received, 10-11, 10-13
RIP statistics
interpreting, 10-12, 10-13
RMON
configuring a mirror port, 19-8, 19-13, 19-19
RMON mirror port configuration parameters
mirror port, 19-11
piggyback port, 19-12
port, 19-11
sampler type, 19-13
RMON statistics
viewing, 19-1, 19-7
robustness variable
IGMP interface parameters, 9-56
IGMP interface statistical parameters, 9-75
LGMP server configuration parameters, 16-25
route add failures
IPX routing table statistic, 12-22
route metric
DVMRP route table parameters, 9-86
route preference by protocol
IP global configuration parameters, 9-14
router cost to source network
DVMRP upstream routers, 9-87
router ID
LSA detail, 11-32
OSPF global configuration parameters, 11-4
OSPF link state database parameter, 11-31
OSPF link state database search parameters, 11-29
OSPF neighbors parameters, 11-26
OSPF statistical parameters, 11-22
OSPF virtual link parameters, 11-15
router is SNMP manageable
DVMRP downstream dependent router, 9-89
router network address
DVMRP downstream dependent router, 9-88
DVMRP upstream routers, 9-87
router port display parameters
application, 16-9
port, 16-9
VLAN, 16-9
router ports, 16-8
router ports removed
IGMP snooping, 16-21
router pruning timer
router pruning timer, 16-7
router received probe from this router
DVMRP downstream dependent router, 9-89
router report time
LGMP server configuration parameters, 16-25
router supports generation ID function
DVMRP downstream dependent router, 9-89
router supports prune function
DVMRP downstream dependent router, 9-89
routing
hardware requirements, 9-2, 12-3
Layer 2 overview, 1-30
Layer 3 (learned) overview, 1-30
Layer 3 (not learned) overview, 1-30
Layer 3 overview, 1-29
routing configuration
minimum requirements, 9-3
Routing with Layer 2 and Layer 3 Modules, 1-29
RTMP RDR Rx
AppleTalk global statistics, 15-26
RTMP RDR Tx
AppleTalk global statistics, 15-26
RTMP Rq Rx
AppleTalk global statistics, 15-26
RTMP Rq Tx
AppleTalk global statistics, 15-26
RTMP Rsp Rx
AppleTalk global statistics, 15-26
RTMP Rsp Tx
AppleTalk global statistics, 15-26
rule number
Layer 3 route cache search parameters, 18-8
running configuration
viewing, 2-46
running.txt, 2-46
RX frame count (T2)
frame forwarding statistical parameters, 18-6


## *S*


sample
Ethernet interface statistical parameters, 19-4

sampler type
port mirroring information parameters, 19-10
RMON mirror port configuration parameters, 19-13
SAP
SAP, 12-4, 12-9
save running configuration to startup configuration
configuration file management, 2-50
saving your current configuration, A-3
search base
LDAP configuration parameters, 9-111
Searching, 6-21
Searching the OSPF Link State Database Using the CLI, 11-32
Searching the OSPF Link State Database Using the Web Agent, 11-27
searching the routing cache, 18-6
Searching the Routing Cache for an Entry, 18-6, 18-9, 18-11
Searching the Switch AFT Using the CLI, 6-21
secondary server
RADIUS configuration parameters, 2-30
secondary server IP address
LDAP configuration parameters, 9-111
secondary server port
LDAP configuration parameters, 9-111
security level
configuring SNMP communities, 2-22
security levels
SNMP, 2-22
seed
AppleTalk interface statistics, 15-28
Select, 9-107
Selecting the Image for Reboot Using the Web Agent, A-6, A-7
sequence
LSA detail, 11-32
OSPF link state database parameter, 11-31
server ID priority
LGMP server configuration parameters, 16-25
service name
IPX service table search parameter, 12-24
IPX static service parameter, 12-15
service port status
event class parameters, 17-17
service ratio (queues), 1-22, 20-1
service type
IPX service table search parameter, 12-24
session ID
multicast session parameters, 16-12
session pruning timer
session pruning timer, 16-7
session search
intelligent multicast, 16-10, 16-13
sessions destroyed
IGMP snooping, 16-21
set recurring
summer time hours, 3-5, 3-8
setting all ports in a module, 5-23
setting summer time hours, 3-4
one time, 3-9
setting switch ports on all modules, 5-36
setting the system clock, 3-2
setting up user accounts, 2-17
severity
event and shutdown log entries, 17-14
shared secret
RADIUS configuration parameters, 2-30
RADIUS secondary server, 2-30
Short PDU in error
AppleTalk global statistics, 15-26
shutdown log
definition, 17-17
shutdown log (switch event)
definition, 17-6
shutdown temperature
temperature threshold parameter, 17-4
size
address table instance hash table parameter, 6-14
SNMP
communities, 2-20
security levels, 2-22
SNMP access level
none, 2-22
read-only, 2-21
read-write, 2-21
read-write with security level set to admin, 2-22
SNMP Administration, 2-20, 2-32, 2-36
SNMP communities, configuring, 2-20, 2-23
access level, 2-21
IP address, 2-21
security level, 2-22
trap receiver, 2-22
SNMP security level
admin, 2-22
normal, 2-22
snmp version supported, 2-20
SNTP
enabling, 3-3, 3-4
socket
IPX service table parameter, 12-25
IPX static service parameter, 12-15
source
IP routing table search parameters, 9-69
IPX route table parameter, 12-21
IPX routing table search parameters, 12-21
IPX service table parameter, 12-25

IPX service table search parameter, 12-24
source address
Layer 3 route cache search parameters, 18-7
source address mask
DVMRP multicast forwarding cache parameters, 9-90
IGMP local multicast forwarding cache parameters, 9-79
source filename
configuration file management, 2-51
source IP address
RADIUS configuration parameters, 2-30
source network
DVMRP route table parameters, 9-86
IPX datagram fields, 12-3
source network mask
DVMRP route table parameters, 9-86
source node
IPX datagram fields, 12-3
source port
Layer 3 route cache search parameters, 18-8
port mirroring information parameters, 19-9
source port number
DVMRP upstream source parameters, 9-92
source socket
IPX datagram fields, 12-3
source subnetwork
DVMRP downstream link parameters, 9-92
DVMRP multicast forwarding cache parameters, 9-90
IGMP local multicast forwarding cache parameters, 9-79
upstream prune information, 9-91
spanning tree
non-VLAN switch port parameters, 5-27
path cost, 4-23
using for setup and monitoring, 4-13
spanning tree bridge level parameters
bridge forward delay, 4-19
bridge hello time, 4-19
bridge max age, 4-19
forward delay, 4-19
hello time, 4-19
max age, 4-19
mode, 4-19
priority, 4-19
spanning tree bridge port
blocking state, 4-22
disabled, 4-22
down state, 4-22
forwarding state, 4-22
learning state, 4-22
listening state, 4-22
spanning tree bridge port information
top change detection, 4-23
spanning tree bridge port information parameters
enable, 4-23
path cost, 4-23
priority, 4-23
spanning tree bridge port parameters
bridge port, 4-21
designated bridge, 4-22
designated cost, 4-22
designated port, 4-22
designated root, 4-22
forward transitions, 4-22
name, 4-21
port, 4-21
state, 4-22
spanning tree bridge ports
configuring, 4-20
spanning tree mode
switch port configuration parameters, 5-29
spanning tree mode for a port, 4-24
Spanning Tree Protocol, 1-7
speed mode
10/100 port parameter, 5-21
SPF hold time
OSPF global configuration parameters, 11-4
SPF runs
OSPF statistical parameters, 11-23
SPF suspend
OSPF global configuration parameters, 11-4
split horizon
RIP interface parameters, 10-5
stale drops
buffer management table parameters, 20-6
STAP mode
switch port parameter, 5-37
start
event class parameters, 17-17
one-time summer time hours configuration, 3-9
summer time hours configuration, 3-7
start network
IPX RIP filter parameters, 13-4
startup config
CPU redundancy configuration, 7-18
startup configuration
viewing, 2-47
startup.txt, 2-46
state
AppleTalk interface statistics, 15-28
AppleTalk route table statistics, 15-29
DVMRP interface statistical parameters, 9-82
IGMP interface statistical parameters, 9-75
IPX SAP interface statistical parameters, 13-8, 14-13
LGMP server display per VLAN parameters, 16-29

OSPF link parameters, 11-24
OSPF neighbors parameters, 11-26
RIP statistical parameters, 10-13
spanning tree bridge port parameters, 4-22
VRRP statistical parameters, 9-102
static
Virtual LAN binding options, 5-31
static address configuration
adding entries to the address forwarding table, 6-21
static client port
creating, 16-18, 16-19
static client ports
deleting, 16-19, 16-20
static multicast session parameters, 16-18
static ext type
OSPF global configuration parameters, 11-4
static low ext type
OSPF global configuration parameters, 11-4
static multicast session configuration parameters
IP address, 16-16
MAC address, 16-16
VLAN, 16-16
static multicast session parameters
IP address, 16-18
MAC address, 16-18
static client ports, 16-18
VLAN, 16-18
static multicast session, creating
creating a static multicast session, 16-15, 16-17
static multicast sessions, configuring
configuring static multicast sessions, 16-17, 16-18
static route
PPP console, 9-115
static route, AppleTalk, 15-11
static routes
IPX
deleting, 12-12
status
address forwarding table parameters, 6-20
CPU redundancy configuration, 7-18
power system statistical parameters, 3-14
stop bits
console serial port settings, 2-34
stub metric
OSPF area parameters, 11-6
summer time hours
one-time setting, 3-9
set recurring, 3-5, 3-8
setting, 3-4
summer time hours configuration
day, 3-8
end, 3-7
hour, 3-8
minutes, 3-8
month, 3-8
recurring, 3-7
start, 3-7
week, 3-7
super age time
definition, 6-9
supervisor module configuration
CLI, 2-4
supported browsers, 2-9
switch
resetting, A-8
switch configuration
managing, 2-48
switch description, 1-1
switch design supported features, 1-14
switch design,definition
MAC Address, 1-14
optional per-VLAN spanning tree, 1-14
segmented address tables, 1-14
switch fabric
event class parameters, 17-18
switch features
crossbar switch fabric,overview, 1-4, 1-6
switch port
configuring, 5-24
switch port configuration
enabling fast start mode, 5-33, 5-34
switch port configuration parameters
3Com mapping table, 5-29
allow learning, 5-29
automatic VLAN creation, 5-28
fast start, 5-29
frame tags, 5-28
hunt group, 5-29
known mode, 5-29
mirror port, 5-29
port VLAN, 5-28
spanning tree mode, 5-29
trunk mode, 5-28
VLAN binding, 5-28
VTP snooping, 5-29
switch port parameters
hunt group, 5-37
links, 5-37
MAC address, 5-37
name, 5-37
port, 5-37
port VLAN, 5-37
STAP mode, 5-37
trunk mode, 5-37
viewing, 5-37
VLAN classification, 5-37
switch ports, single command, 5-36

Synchronizing the Primary and Redundant CPUs, 7-14
system
event class parameters, 17-17
system information
editing, 3-2
system information, changing
contact, 3-2
location, 3-2
system reset
performing, 3-16

# *T*

TblInst
address forwarding table parameters, 6-19
TCP established
IP access list parameters, 9-27
TCP/UDP destination port
IP access list parameters, 9-27
TCP/UDP source port
IP access list parameters, 9-27
Technical Support
contacting, -xv
technical support
contacting, -xv
temperature status
event class parameters, 17-17
viewing, 17-2
temperature system
configuring, 3-12, 3-13
temperature threshold parameters
low shutdown temperature, 17-4
lower warning temperature, 17-4
shutdown temperature, 17-4
upper warning temperature, 17-4
temperature thresholds, 17-4
terminal setup, 2-2
TFTP server
copying, 2-51
TFTP server IP address
configuration file management, 2-51
TFTP transfer status
viewing, 2-53
this router is group membership querier
IGMP interface statistical parameters, 9-75
Throughput, 1-5, 1-7
ticks
IPX RIP filter parameters, 13-5
IPX route table parameter, 12-22
IPX static route, 12-11
time of state change
VRRP statistical parameters, 9-102
time stamp
event and shutdown log entries, 17-14
times this VR became master
VRRP statistical parameters, 9-102
too long
AppleTalk global statistics, 15-26
too short
AppleTalk global statistics, 15-26
top change detection
spanning tree bridge port information, 4-23
T-option
OSPF neighbors parameters, 11-27
total entries
forwarding cache (FE) parameters, 18-11
total number of entries
address table instance parameters, 6-13
total routes added
IP routing table statistical parameters, 9-71
total routes deleted
IP routing table statistical parameters, 9-71
total system power
power system statistical parameters, 3-14
trace
protocol event log settings, 17-12
traffic flooding, 19-8
traffic mirror port, 19-11
transit delay
OSPF interface parameters, 11-11
OSPF virtual link parameters, 11-15
translate 7 into 5
OSPF area parameters, 11-6
transport control
IPX datagram fields, 12-2
trap receiver
configuring SNMP communities, 2-22
triggered updates
IPX SAP interface parameters, 14-2
RIP global configuration parameters, 10-3
triggered updates sent
IPX SAP interface statistical parameters, 13-9, 14-14
RIP statistical parameters, 10-13
trunk mode
Cisco Catalyst 5000, parameters, 5-30
switch port configuration parameters, 5-28
switch port parameter, 5-37
TTL
AppleTalk ARP cache table statistics, 15-32
IPX route table parameter, 12-21
IPX service table parameter, 12-25
purge, 10-2
TTL expired
AppleTalk global statistics, 15-26
TTY console settings
baud rate, 2-34
data bits, 2-34

flow control, 2-34
parity, 2-34
stop bits, 2-34
tunnel endpoint address
DVMRP interface parameters, 9-60
type
AppleTalk ARP cache table statistics, 15-32
AppleTalk NBP filter parameters, 15-17
AppleTalk NBP table parameters, 15-35
AppleTalk static route, 15-13
AppleTalk zone filter parameters, 15-21
DVMRP interface statistical parameters, 9-82
event and shutdown log entries, 17-14
forwarding cache (FE) parameters, 18-11
IPX SAP filter parameters, 14-6
IPX SAP network filter parameters, 14-10
IPX service table parameter, 12-25
IPX static service parameter, 12-15
LSA detail, 11-32
multicast session parameters, 16-12
OSPF link parameters, 11-24
OSPF link state database parameter, 11-30
OSPF link state database search parameters, 11-29
power system statistical parameters, 3-14
type 20 packet propagation
IPX interface, 12-9
type 3 ASE filter
OSPF area parameters, 11-6

## *U*

UDP in datagrams
IP routing global statistics, 9-67
UDP in errors
IP routing global statistics, 9-67
UDP out datagrams
IP routing global statistics, 9-67
UDP port
RADIUS configuration parameters, 2-31
undersize packets
Ethernet interface statistical parameters, 19-6
unknown messages codes encountered
DVMRP global statistical parameters, 9-80
unknown messages received
IGMP global statistic parameters, 9-74
IGMP interface statistical parameters, 9-76
unrecognized packets received
DVMRP interface statistical parameters, 9-82
UPD in no ports
IP routing global statistics, 9-67
update pkt delay
RIP global configuration parameters, 10-3
update timer
RIP global configuration parameters, 10-2
update timestamp
VTP snooping parameters, 4-49
updater identity
VTP snooping parameters, 4-49
updater time stamp
VLAN exchange parameters, 4-49
updates received
IPX SAP interface statistical parameters, 13-9, 14-14
RIP statistical parameters, 10-11, 10-13
upper warning temperature
temperature threshold parameter, 17-4
upstream interface
DVMRP multicast forwarding cache parameters, 9-90
IGMP local multicast forwarding cache parameters, 9-79
upstream interface is pruned
DVMRP multicast forwarding cache parameters, 9-91
upstream neighbor router address
DVMRP multicast forwarding cache parameters, 9-90
upstream prune information
destination group address, 9-91
DVMRP upstream interface, 9-91
interface is pruned, 9-91
interface type, 9-91
prune expiration time, 9-91
source subnetwork, 9-91
upstream router
DVMRP route table parameters, 9-86
upstream source
IGMP local multicast forwarding cache parameters, 9-79
upstream sources, 9-92
DVMRP multicast forwarding cache parameters, 9-91
use default route
use default route, 12-4
use default route for proxy ARP
IP global configuration parameters, 9-13
use interpacket gap
IPX SAP interface parameters, 14-2
use max packet size
IPX SAP interface parameters, 14-2
user accounts
setting up, 2-17
user logins
default, 2-17
user port status
event class parameters, 17-17
using dial-up networking
using dial-up networking, 2-42

Using Note, Caution, and Warning, -xviii
Using the Web Agent, 16-8
utilization
Ethernet interface statistical parameters, 19-4

## V

valid
address forwarding table parameters, 6-19
version
RIP interface parameters, 10-5
view the active alarm table, 17-5, 17-6
Viewing, 9-113
viewing AppleTalk global statistics, 15-24, 15-27
Viewing AppleTalk Global Statistics Using the CLI, 15-27
viewing AppleTalk route table statistics, 15-30
viewing AppleTalk statistics, 15-24
viewing AppleTalk zone table statistics, 15-33, 15-34
viewing DVMRP downstream routers, 9-88
viewing DVMRP neighbor routers, 9-83
viewing DVMRP upstream routers, 9-87
viewing Ethernet statistics, 19-1, 19-7
viewing event and shutdown logs, 17-12, 17-15
viewing event statistics, 17-15, 17-16, 17-18, 17-19
viewing IGMP interface statistics, 9-74, 9-76
Viewing LDAP Statistics, 9-113
viewing RMON statistics, 19-1, 19-7
viewing switch port parameters, 5-37
Viewing Switch Port Parameters Using the CLI, 5-38
viewing the AppleTalk ARP cache table, 15-31, 15-32
viewing the AppleTalk NBP table, 15-34, 15-35
Viewing the AppleTalk Route Table, 15-28
viewing the AppleTalk route table, 15-29
viewing the AppleTalk zone table, 15-33
viewing the downloaded image, A-6
viewing the running configuration, 2-46
viewing the script execution log file
script execution log file
viewing, 2-47
viewing the startup configuration, 2-47
Viewing the Status of a TFTP Transfer, 2-53
viewing the TFTP transfer status, 2-53
viewing VRRP statistics, 9-100, 9-102
Virtual, 1-14
Virtual Bridging Functions, 1-14
Virtual LAN binding options
bind to all, 5-31
bind to received, 5-31
static, 5-31
Virtual LANs
binding options, 5-31
flood pruning overview, 1-15
trunk mode, configuring, 5-26
virtual LANs
creating a VLAN, 4-8, 4-10
parameters, 4-9
Virtual LANs, configuring
automatic VLAN creation, 5-27
trunk mode, 5-26
VLAN binding, 5-27
virtual router
VRRP, 9-96, 9-100
VLAN
add IP interface parameters, 9-7
AppleTalk interface parameters, 15-6
ARP cache search parameters, 9-72
configuring all ports, 4-11
creating, 4-8, 4-10
egress rules, 4-7
filtering, 6-16
forwarding rules, 4-5
IPX interface, 12-8
Layer 3 route cache search parameters, 18-8
LGMP client display per VLAN parameters, 16-34
LGMP server display per VLAN parameters, 16-28
multicast session parameters, 16-12
operation, 4-4
router port display parameters, 16-9
search, 6-16
static multicast session configuration parameters, 16-16
static multicast session parameters, 16-18
VLAN association
address table instance parameters, 6-13
VLAN binding
Cisco Catalyst 5000 parameters, 5-30
switch port configuration parameters, 5-28
VLAN binding, configuring
Virtual LANs, 5-27
VLAN classification
switch port parameter, 5-37
VLAN configuration parameters
auto increment HT size, 4-10
initial hash table size, 4-10
VLAN considerations, 4-7
VLAN exchange parameters
updater timestamp, 4-49
VLAN operation
ingress rules, 4-4
VLAN Operational Rules, 5-5
VLAN spanning tree bridge level parameters
bridge forward delay, 4-19
bridge hello time, 4-19
bridge max age, 4-19
forward delay, 4-19
hello time, 4-19

max age, 4-19
mode, 4-19
priority, 4-19
VLAN switch port table parameters
binding type, 4-12
frame format, 4-12
port, 4-12
port name, 4-12
VLAN trunking,definition, 1-10
VR ID
VRRP configuration parameters, 9-98
VRRP statistical parameters, 9-101
VRRP
add IP interface parameters, 9-9
enabling, 9-93
IP global configuration parameters, 9-13
VRRP configuration overview, 9-93
VRRP configuration parameters
addr owner override, 9-100
advertisement timer, 9-99
auth key, 9-99
interface, 9-98
IP address, 9-98
priority, 9-98
VR ID, 9-98
VRRP overview
configuring, 9-93
VRRP router
creating, 9-96
VRRP statistical parameters
advertisements received, 9-102
advertisements sent, 9-102
bad advertisements received, 9-102
interface, 9-101
IP address, 9-101
state, 9-102
time of state change, 9-102
times this VR became master, 9-102
VR ID, 9-101
VRRP statistics
viewing, 9-100, 9-102
VRRP virtual router
creating, 9-96, 9-100
VTP snooping
Cisco Catalyst 5000 parameters, 5-30
VTp snooping
switch port configuration parameters, 5-29
VTP snooping parameters
configuration revision number, 4-48
domain name, 4-48
update timestamp, 4-49
updater identity, 4-49
VTP snooping state, 4-48
VTP snooping state
VTP snooping parameters, 4-48

## W

warning
protocol event log settings, 17-11
Web Agent
logging into, 2-9
setting up user accounts, 2-17
week
summer time hours configuration, 3-7

## X

Xon/Xoff
flow control, 2-34

## Z

Zip Ext Reply Rx
AppleTalk global statistics, 15-26
Zip Ext Reply Tx
AppleTalk global statistics, 15-27
Zip GNI Rq Rx
AppleTalk global statistics, 15-27
Zip GNI Rq Tx
AppleTalk global statistics, 15-27
Zip GNI Rsp Rx
AppleTalk global statistics, 15-27
Zip GNI Rsp Tx
AppleTalk global statistics, 15-27
Zip Query Rx
AppleTalk global statistics, 15-26
Zip Query Tx
AppleTalk global statistics, 15-26
Zip Reply Rx
AppleTalk global statistics, 15-26
Zip Reply Tx
AppleTalk global statistics, 15-26
zone
AppleTalk interface parameters, 15-7
AppleTalk NBP table parameters, 15-35
AppleTalk static route, 15-13
zone filter
adding interfaces, 15-23, 15-24
creating, 15-20
deleting interfaces, 15-23, 15-24
editing, 15-22
zones
AppleTalk route table statistics, 15-30